NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE
and
SCHOOL OF INFORMATION WARFARE AND STRATEGY

# TOWARD A NATIONAL ENCRYPTION STRATEGY

May 25, 1998

MICHAEL H CAMILLETTI / CLASS OF 1998

Directed Research
Course 5490

FACULTY RESEARCH ADVISORS
Dr S Botsai, NWC
Dr D Kuehl, SIWS

FACULTY ADVISORS
Mr J Stefan, NWC
Mr T Czerwinski, SIWS

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **25 MAY 1998** | | **25-05-1998 to 25-05-1998** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Toward a National Encryption Strategy** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National War College,300 5th Avenue,Fort Lesley J. McNair,Washington,DC,20319-6000** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**see report**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | | **183** | |

## Disclaimer and Copyright Notices

## Preface

The current administration is struggling with the failures and challenges of advocating policy for encryption technology uses, both domestically and for export, because it neglected to develop a vision of what encryption uses meant to legitimate users, focusing instead upon threats raised by those who exploit encryption technology and how that impacted U S interests There are conflicts within the administration among the Departments of Commerce, Justice, and Defense as well as within the Intelligence Community The potential for legislated solutions supercedes the administration's aims Business and commercial interests coupled with individual fears about government intrusion into an area of personal freedom challenge any government intrusion It appears now that no adequate compromises can be found A National Encryption Strategy can provide some relief

In the study of national security Strategy (with the big 'S') precedes policy which in turn leads to implementation or an implementing strategy (with the little 's') This concept and the framework that go with it can provide a guide to solving the current challenges regarding encryption technology controls

In this paper, I have attempted to report the current dilemma, identify the participants and their views, analyze the issues, and propose such a Strategy If successful, this approach can provide the administration a fresh perspective on the issues and a means of selecting compatible policies for the variety of areas that are affected by encryption technology

ACKNOWLEDGMENTS

The author acknowledges several individuals for their contributions to this report

Doctor Sarah Botsai, Doctor Daniel Kuehl, Mr James Stefan, and Mr Tom Czerwinski who served as my advisor team at the National War College and the School of Information Warfare and Strategy Their patience and criticism helped mold this report into a better form Doctor Albert Pierce and Doctor Thomas Keaney who provided detailed critiques of my other writing projects in such a constructively positive way as to improve the quality of this project They also provided the framework for strategy formulation from which I could attempt to analyze the current policy debate about encryption and articulate my proposed strategy

The Honorable William Reinsch, Doctor Clinton Brooks, Mr John Marvita, and Ms Shari Steele for insightful and cooperative discussions about encryption policy dilemmas and current actions underway to address these problems

Melinda Edwards who was a stalwart friend and idea sounding board during the term The members of Committee 7 Barbara Cummings, John Custer, Geo Davis, Ginni Farris, Tony Fortune, Tom Griffith, Blair Hansen, Joe Krauss, Anne Leary, Zul Mazlun, Phil Pope, Rick Rushton, John Schmidt, and Kim Welliver They had to put up with me every day Finally, the faculty and staff of the National Defense University for providing the climate that permitted so much academic richness

Table of Contents



---

**CLIPPER CHIP**, A Policy Challenge of the Information Age

**National Security, Law Enforcement, and the Freedom to be Left Alone:** *What's Happening in the Encryption Debate?*

**The President's Commission on Critical Infrastructure Protection** The Need for a National Infrastructure Assurance Agency

**A National Strategy for Encryption Technology**

A Framework for Global Electronic Commerce, July 1997

Administration Statement on Commercial Encryption Policy, July 1996

## EXECUTIVE SUMMARY

### Issue

The Clinton Administration has articulated at least three potential policies in the past six years attempting to define appropriate limits and controls on the sale and use of encryption products by business and individuals outside of government itself[1] Additionally, the Congress has taken up the issue of encryption technology control with several bills ( one remains in the House and two remain in the Senate) during the 1997 session alone As this is being written, a current administration policy has lost a defining case in Federal District Court[2], one liberalizing bill in the House is foundering in committee, one in the Senate is stopped dead, and a consortium of business and private interests is launching attacks on many fronts against both the executive and legislative branches' efforts to define policy and law Additionally, the Presidential Committee for Critical Infrastructure Protection (PCCIP) has endorsed the concept of key escrow in its November 1997 report (chapter 1) This, however, directly contradicts the conclusions of several government reports, i e , the National Research Council (May 1996), the Office of Technology Assessment (January 1994), and the GAO (March 1995) and gives credibility to the idea that the administration has no coherent basis for establishing policy

In all there are perhaps 21 unique groups that stand to benefit or suffer from the outcome of

[1] See Appendix D A Chronology of the Cryptography Issues

[2] Bernstein v Department of State, see text p 14

the encryption technology control debate and the subsequent policy formulation Each has a set of interests that often coincide and sometimes conflict with the interests of other groups Many are represented by the same or similar lobbying bodies as the issue is debated in Congress and among the administration's various agencies

Simplicity in framing the analysis of each group's views suggests that the following framework will be useful in the remainder of this summary The nexus of the debate pits individuals ( including academics) and business on one side (favoring the least restrictive policies) against the executive branch agencies for national security and law enforcement on the other The Executive Office of the President, the Congress, and the Courts represent interests between these extremes Foreign interests, both government and private, are secondary as the U S policy debate unfolds

**Facts**

- Encryption products capable of key lengths up to at least 128 bits (strong) are available
- Export controls adjudicated by the Department of Commerce limit exportable encryption products to 40 bit key lengths Some exceptions for Digital Encryption Standard (DES) products (56bits) and special case by case exceptions for multinational businesses with U S corporate charters are granted
- Law enforcement officials want to restrict all domestic and export encryption products to those providing key recovery (see glossary) capabilities
- NSA seeks to both promote strong encryption domestically and to preserve existing export controls
- Congress considered several bills in 1996 and 1997 that either restrict encryption technology (as the FBI wishes) or promote the free market deployment of strong

encryption products without restrictions (as privacy advocates and business wish)

- The 9th Circuit Court of Appeals heard arguments to overturn a lower court ruling that struck down government controls on the export of long key length encryption source code (the plain text, line by line written version of software)

**Arguments**

Privacy

As pertains to the possession, use, and distribution of encryption technologies, the 4th and 5th Amendment proscription against searches, seizure, taking, and incrimination provide probably the strongest support to the individual argument against encryption controls Inasmuch as any law restricting the use of encrypted matter prevents a citizen from enjoying freedom from unreasonable government intrusion, it is probably a violation of these amendments On its face, the use of encryption is no different from the use of a front door When it is open, it invites those outside to peer within But once it is shut, it prevents those outside from any certain knowledge of what is within

Business

Electronic commerce, the topic common to private and commercial interests, provides the most compelling reason to lift U S export restrictions Safe electronic transactions are a must Shared encryption is the enabling technology that will permit this to happen Export restrictions slow the growth not only of electronic commerce, but global economic development all together, some argue Therefore, the promotion of global commerce demands a corresponding support for the mechanisms that enhance such growth

National Security

The National Security Agency is of two minds It maintains that the use of domestic public cryptology is not harmful to national security It also wishes to reserve the current export controls to prevent foreign users from obtaining strong encryption capabilities Privately, the spread of encryption is less daunting to the NSA mission than its public statements indicate

Exploiting the contents of intercepted signals is the single most important aspect of cryptology Nonetheless, much can be learned without resorting to deciphering intercepted traffic into plain text Rejection of encrypted traffic based on knowledge of the source often obviates the need to decode at all [3]

Ultimately, foreign threats to U S security can obtain strong encryption without resorting to commercial sales or U S sources It is inexpensive to hire a software engineer to write source code for encryption schemes The NSA must deal with strong encryption no matter what results from the current debate While the NSA might remain ambivalent toward commercial applications, it seems to have limited arguments that favor restrictions

## Law Enforcement

What role should law enforcement play in the encryption debate? Advocates for a strong role argue that crime prevention is a primary function of the federal law enforcement community To accomplish this it requires broad powers to interdict potential crimes before they are committed Encryption of conversations and documents hinders this, the FBI claims

Regardless of the obstacle encryption might pose, before the FBI can obtain a legal wiretap or electronic surveillance it must present compelling evidence that a crime is imminent It must apply

[3] Whitfield Diffie and Susan Landau, Privacy on the Line, MIT Press, January 1998 Also personal communication with NSA by the author The National Research Council report dated May 1996 hints at this conclusion as does the Hoffman work, DE-AC05-840R21400

for a warrant through a supervisor, a Deputy Assistant Attorney General, and a Federal Judge But, if the FBI can convince these persons that a crime is imminent, their encounter with encrypted communications should not destroy the case The timing of evidence collection and analysis and the scheduling of an arrest might become problematic, but that is another matter Simply put, evidence of a conspiracy to commit a crime seldom originates as a result of electronic surveillance The surveillance in fact cannot exist until evidence of a crime precedes it So the crime prevention portion of the FBI's argument is weak

A stronger argument can be made in the case of criminal investigation In these cases some criminal act has already occurred and the FBI is obtaining evidence from a variety of sources Physical and forensic evidence make the most compelling evidence Witness statements, accomplice confessions, photography and video are also strong Phone records, computer files and recorded conversations are important, but less so If these latter are encrypted, it does indeed hurt the mission of the FBI in solving a crime Historic records indicate that surreptitiously gathered communications are seldom used and less often critical to prosecuting criminal cases [4]

---

Law enforcement agencies have a mixed record of properly using wiretap and electronic surveillance permission Numerous cases show a disregard for non targeted individuals' privacy, subsequent blackmail, and, perhaps worse, obtaining wiretap authority by false pretenses The

---

[4]A. Michael Froomkin, The Metaphor is the Key. Cryptography, the Clipper Chip, and the Constitution, The University of Pennsylvania Law Review, January 1995
Froomkin and others, notable Whitfield Diffie and Susan Landau document cases of FBI abuses Two ideas stand out The FBI requests large numbers of wiretaps and surveillance approvals that generate little or no evidence It appears this technique is used to "cover the bases" of a widely cast net to see what gets caught Second, there is no case where an encrypted piece of evidence prevented law enforcement from proceeding with a case Louis Freeh, in his congressional testimony, cited 4 cases (of the 9000 some wiretaps reviewed since 1990) Each was shown to be false

status quo provides law enforcement agencies with great powers for intrusion into private areas To include guaranteed decryption capability for law enforcement raises the possibility of abusing innocent persons liberties in the pursuit of evidence gathering

**Findings**

Encryption is available Individuals and businesses have the wherewithal to obtain or to write for themselves effective encryption schemes privately or to buy them commercially Private versions prevent widespread uses such as insuring Internet security or protecting e-mail The owner must deliver a secure copy of the scheme to the recipient prior to any encrypted communication It is, however, a possibility that many companies can choose if avoiding key recovery schemes is important It is also the alternative that U S businesses fear will be employed by competing foreign business interests Finally, it is the likely alternative criminals will use if key recovery is required for commercial systems

If the policy or law enacted requires key recovery for encryption controls, judges are likely to support the constitutionality of such measures Michael Froomkin's analysis (chapter 2) indicates that such measures are not intrusive enough to merit judicial protection of individual freedoms Protection of the public safety tends to over ride personal freedoms in the federal courts

Business interests in the free market deployment and use of commercial products to support secure electronic commerce might, however, tip the scale against key recovery schemes There is a strong pro-business element in both the administration and the Congress toward promoting economic activity

Individuals concerned with personal privacy will probably have to live with whatever business and government eventually agree to do A compromise between business interests and the

government is most likely since economic impacts are readily calculated and directly felt by politicians This can work for individual rights, however, since most of the aims of business coincide with individual concerns

Law enforcement will continue to receive wiretap and electronic surveillance approvals under the current law without regard to the encryption issue If they succeed in obtaining key recovery provisions, business and individual freedoms will suffer, but actual losses to personal freedoms are unlikely to be greater than what is now the case

**Proposal**

If software developers agreed to escrow not the keys, but the source codes of their products and in return received unrestricted freedom to export strong encryption worldwide while pursuing free market strategies for their products, a smaller trusted agency would be capable of maintaining the proprietary interests of businesses(similar to patent and copyright protections) while acting as the gatekeepers for national security or law enforcement access to these source codes Source codes themselves do not guarantee successful decryption, but according to NSA spokespersons, contribute toward reducing the burden of decryption efforts

Separation of interests between law enforcement and trusted agents would be inherent But armed with judicial approval, law enforcement could access the source code from the escrow location and use it to assist in the code breaking , if this became necessary during the pursuit of a potential criminal enterprise While not providing instant decoding capability, NSA experts agree that access to the source code provides, "things we can work with "[5] If NSA could then share this expertise with law enforcement agencies, a potential to protect privacy while assisting law

[5] Personal communication with NSA personnel

enforcement interests exists

Additionally, to fund this approach, a software sales surcharge can be imposed on buyers of encryption products Set at an amount fair to the buyer and capable of funding the trusted system, it might amount to $1 to $5 per sale This could generate substantial sums over time to provide law enforcement with enhanced tools to collect and analyze suspect communications

This approach preserves the freedom of individuals while permitting choice, but with the voluntary recognition that this freedom indeed has a cost It promotes world markets for business It addresses law enforcement concerns, albeit to a lesser degree than law enforcement wishes But approaching the degree to which the documented problem actually exists

## Glossary and Acronym Expansion

ALGORITHM
A mathematical procedure that can usually be explicitly encoded in a set of computer language instructions that manipulate data Cryptographic algorithms are mathematical procedures used for such purposes as encrypting and decrypting messages and signing documents digitally

BIT
Short for binary digits--0 or 1 Keys are strings of bits

CELLULAR TRANSMISSION
Data transmission via interchangeable wireless (radio) communications in a network of numerous small geographic cells Most current technology is analog--represented as electrical levels, not bits However, the trend is toward digital cellular data transmission

CIA - Central Intelligence Agency

CLIPPER CHIP
A microcircuit that contains a classified secret-key encryption algorithm--"Skipjack " Skipjack can be used in place of DES, RC2, RC4, and other secret-key algorithms to provide message privacy with a "key-escrow" system (The administration initially referred to the microcircuit as the Clipper Chip and later discontinued using the term )

COCOM
The Coordinating Committee for Multilateral Export Controls--an informal organization that cooperatively restricts strategic exports to controlled countries COCOM consists of 17 countries that maintain three export control lists (1) the International Industrial List, (2) the International Munitions List, and (3) the International Atomic Energy List Members include the countries of the North Atlantic Treaty Organization, except Iceland, with the addition of Japan and Australia

CRYPTOLOGY
The transformation of ordinary text, or "plain text," into coded form by encryption and the transformation of coded text into plain text by decryption Cryptology can be used to support digital signature, key management or exchange, and communications privacy

DATA ENCRYPTION STANDARD (DES)
A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data and performing other functions For example, DES can be used to check message integrity DES specifies a key length of 56 bits

DIGITAL SIGNATURE
A cryptographic method, provided by public-key cryptography, used by a message's recipient or any third party to verify the identity of the message's sender and the integrity of the message A sender creates a digital signature or a message by transforming the message with his/her private key A recipient, using the sender's public key, verifies the digital signature by applying a corresponding transformation to the message and the signature

DIGITAL SIGNATURE STANDARD (DSS)
A NIST-proposed Federal Information Processing Standard that supports digital signature

DIGITAL TELEPHONY
Telephone systems that use digital communications technology

ECONOMIC ESPIONAGE
The unauthorized acquisition of U S proprietary or other information by a foreign government to advance the economic position of that country

ENCRYPTION
The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage Encryption is based on an algorithm and at least one key Even if the algorithm is known, the information cannot be decrypted without the key(s)

FIPS - Federal Information Processing Standard

IBM - International Business Machines, Inc

INFORMATION-PROCESSING STANDARD
A set of detailed technical guidelines used to establish uniformity to support specific functions and/or inter-operability in hardware, software, or telecommunications development, testing, and/or

operation

INTEGRATED SERVICES DIGITAL NETWORK
An emerging communications system enabling the simultaneous transmission of data, facsimile, video, and voice over a single communications link

INTEROPERABILITY
The ability of computers to act upon information received from one another

KEY
A long string of seemingly random bits used with cryptographic algorithms to create/verify digital signatures and encrypt/decrypt messages and conversations The keys must be known or guessed to forge a digital signature or decrypt an encrypted message

KEY-ESCROW SYSTEM
An electronic means of reconstructing a secret key (for secret-key encryption) or a private key (for public-key encryption) The reconstructed key can then be used in a process to decrypt a communication

KEY MANAGEMENT/EXCHANGE
A method of electronically transmitting, in a secure fashion, a secret key for use with a secret-key cryptographic system Key management can be used to support communications privacy This method can be accomplished most securely with public-key cryptographic systems, which do not require the sharing of secret keys with third parties Instead, a secret key is encrypted with a recipient's public key, and the recipient decrypts the result with his/her private key to receive the secret key A variation of key management that is based on key exchange does not require encrypting the secret key

MASS-MARKET SOFTWARE
Software that is (1) generally available to the public by sale, without restriction, from stock at retail selling points through over-the-counter, telephone, and mail transactions and (2) designed for user installation without substantial supplier support

NIST - National Institute of Standards and Technology

NSA - National Security Agency

NSDD - National Security Decision Directive

OSI - Office of Special Investigations, GAO

PCCIP- Presidential Commission for Critical Infrastructure Protection

PERSONAL COMMUNICATIONS NETWORK
Advanced cellular telephone communications and the interworking of both wired and wireless networks that will offer new communications services via very small, portable handsets The network will rely on micro cellular technology--many low-power, small-coverage cells--and a common channel-signaling technology, such as that used in the telephone system, to provide a wide variety of features in addition to the basic two-way calling service

PRIVATE KEY
The undisclosed key in a matched key pair--private key and public key--that each party safeguards for public-key cryptography

PUBLIC KEY
The key in a matched key pair--private key and public key--that may be published, e g , posted in a directory, for public-key cryptography

PUBLIC-KEY CRYPTOGRAPHY
~~Cryptography using two matched keys (or asymmetric cryptography) in which a single private key is not shared by a pair of users~~
Instead, users have their own key pairs Each key pair consists of a matched private and public key Public-key cryptography can perform (1) digital signature, (2) secure transmission or exchange of secret keys, and/or (3) encryption and decryption Examples of public-key cryptography are DSS and RSA

RC2, RC4 (RIVEST CIPHER 2 AND RIVEST CIPHER 4)
Two secret-key encryption systems that are implemented in mass-market software These systems are proprietary and are marketed by RSA Data Security, Inc RC2 and RC4 can be used with various key lengths, such as 40 bits or 56 bits

RSA
A public-key algorithm invented by Ronald L Rivest, Adi Shamir, and

Leonard M Adleman RSA can be used to generate digital signatures, encrypt messages, and provide key management for DES, RC2, RC4, and other secret-key algorithms RSA performs the key-management process, in part, by encrypting a secret key for an algorithm such as DES, RC2, or RC4 with the recipient's public key for secure transmission to the recipient This secret key can then be used to support private communications

SECRET KEY

The key that two parties share and keep secret for secret-key cryptography Given secret-key algorithms of equal strength, the approximate difficulty of decrypting encrypted messages by brute force search can be measured by the number of possible keys For example, a key length of 56 bits is over 65,000 times stronger or more resistant to attack than a key length of 40 bits

SECRET-KEY CRYPTOGRAPHY

Cryptography based on a single key (or symmetric cryptography) It uses the same secret key for encryption and decryption Messages are encrypted using a secret key and a secret-key cryptographic algorithm, such as Skipjack, DES, RC2, and RC4

SKIPJACK

A classified 64-bit block encryption, or secret-key encryption, algorithm The algorithm uses 80-bit keys (compared with 56 for DES) and has 32 computational rounds or iterations (compared with 16 for DES) Skipjack supports all DES modes of operation Skipjack provides high-speed encryption when implemented in a Clipper Chip (initial name)

TRAPDOOR

A secret entry point to a cryptographic algorithm through which the developer or another entity can bypass security controls and decrypt messages

VPN

Virtual Private Network

WIRETAPPING

The real-time collection of transmitted data, such as dialed digits, and the sending of that data in real time to a listening device ("Real time" is defined as the actual time that something, such as the communication of information, takes place )

# INTRODUCTION

## Why a National Strategy for Encryption Technology is needed.

Two things are clear everybody says the Information Age is a marvelous thing, nobody agrees on how to go about living it All else is chaos But this is the kind of chaos that Americans thrive on Government has provided a gift -- the information superhighway The Internet was born from a network of 1970's computer systems wired by dedicated communications lines among universities, government laboratories, and private contractors doing business with the government. With the invention of the high speed router (by a married couple, both employed at a government lab but in different offices, who wished to communicate with each other at work) the fundamental hardware of the system was in place The Computer Revolution of the 1980's provided the "desktop on every desk" environment that generated the market for electronic communication by data, voice, and e-mail among businesses, government and individuals And Bill Gates invented Microsoft Corporation with its propensity for developing the software that ran the show Somewhere, as the 80's gave way to the 90's, the concept and practice of "going on-line" caught on Commercial interests developed and provided low cost, effective products that in turn spawned both consumer demand and corporate recognition that the Internet was the locus of the Information Revolution By 1997, an estimated 50 million Americans and some 80 million people worldwide were doing everyday activities from banking to shopping to "calling home" via the worldwide web, the electronic marketplace, or the e-mail link [6]

It is inevitable, then, that the government would have a challenge in promoting a variety of sometimes conflicting aims and of adjudicating among often conflicting interests The Constitution

[6] Estimate provided by CNET (Http //www cnet com)

empowers the Federal Government with the regulation of commerce, the provision of National Defense, the promotion of public safety, and the protection of personal liberties [7] Today, however, the government is beset by challenges in administering these responsibilities A series of policies and regulatory efforts about electronic issues have been met with fierce opposition, infighting among disparate agencies, and court challenges As these battles unfold, it becomes clear that the administration's commitment to promoting the Information Age is not developing well Policies in one area are found to contradict law, regulation, or other policies from other areas of government Promoting commerce interferes with protecting public safety national security interests interfere with the global economic interests we need to pursue Protecting liberty raises the risks to innocent persons of violent actions by those who can exploit technology for their own aims Conflicting policies reflect these conflicting aims and values from among the variety of persons and organizations who have made the transition into electronic means of daily living

Perhaps the most compelling example of government policies that are caught in the inter-tangled web of conflict among various groups is the current debate about encryption technology Encryption is, of course, one part of a larger whole that involves cryptology, the science of encoding and decoding data [8] That in turn is a small part of the overarching area described as electronic commerce which, paradoxically, provides the umbrella conceptual framework for all non governmental uses of electronic information transmission and storage personal, private

[7] George Washington, et al, Constitution of the United States of America, 1787 reprinted by The Institute for National Strategic Studies, National Defense University Press, U S GPO, Washington, DC, 1985

[8] see Glossary

business, and commercial [9] Elements of encryption include digital signatures which promote the non repudiation of electronic documents, authenticity certification which promotes the validity of transmitted data, and data security which promotes the protection from unauthorized or unintended view of sensitive information by others

The administration has articulated at least three potential policies in the past six years attempting to define appropriate limits and controls on the sale and use of encryption products by business and individuals outside of government itself [10] Additionally, the Congress has taken up the issue of encryption technology control with several bills ( one remains in the House and two remain in the Senate) during the 1997 session alone As this is being written, a current administration policy has lost a defining case in Federal District Court[11], one liberalizing bill in the House is foundering in committee, one in the Senate is stopped dead, and a consortium of business and private interests is launching attacks on many fronts against both the executive and legislative branches' efforts to define policy and law Additionally, the Presidential Committee for Critical Infrastructure Protection (PCCIP) has endorsed the concept of key escrow in its November 1997 report This, however, directly contradicts the conclusions of several government reports, i e , the National Research Council (May 1996), the Office of Technology Assessment (January 1994), and the GAO (March 1995) and gives credibility to the idea that the administration has no coherent basis for establishing policy

These factors lead to the conclusion that a National Strategy is needed to promote and control

[9] See Appendix B A Framework for Global Electronic Commerce

[10] See Appendix D A Chronology of the Cryptography Issues

[11] Bernstein v Department of State, see text p 14

the use of encryption technology in the electronic infrastructure of government, business, and personal activities There are, it would seem, five areas of policies that need an over arching Strategy to provide consistency among them First, national security considerations, particularly our ability to defeat foreign encryption efficiently, must be preserved Second, the promotion of U S business interests in global markets, including the exporting of U S developed software encryption products should be enhanced. Third, the freedom to conduct academic research and the implied freedom to share the fruits of such work (with contemporaries) is essential to advancing the science of cryptology Fourth, the protection of individual freedoms, including the desire of persons to conduct their lives privately and safely must be advanced Finally, the desire of law enforcement to detect criminal activity using advanced electronic methods, such as encryption, should be accommodated While these areas are not listed in any particular order, the pursuit of any policy necessarily prioritizes these interests It is clear that some conflicts will exist among them This makes clear the need for either a compromise solution (which does not always provide good policy) or a selection process that minimizes the potential risk while setting priorities

A framework for defining such a strategy would include identification of national, business, and private interests that are impacted by the result, a description of the environment in which the strategy must operate, a review of the resources available to pursue a particular strategy, an analysis of the risks and costs of pursuing alternative strategies, and a proposal for implementing a strategy Once such an effort was concluded, the government would have a "touchstone" from which a variety of policies could be defined and conflicts ameliorated That is the aim of this study

Chapter 1 reports the issues as they exist today It provides a chronology of critical events and identifies the various groups involved in the debate Chapter 2 analyzes the stakeholders' arguments and attempts to balance the emotional nature of this debate with a factual review of the key points made by each group Chapter 3 proposes a strategy that can accommodate the conflicting aims of the competing interest groups and permit the administration to move forward with a series of compatible policy initiatives that both address encryption issues and fit into the larger framework of electronic commerce Appendix A provides a brief tutorial about how public key encryption works Appendices B and C provide copies of the two pivotal policy statements made by the White House during 1996 and 1997 that paradoxically establish the vision of an open electronic environment while restricting its utility with government controls Appendix D is a chronology of the cryptology issues Also included are a series of articles that define portions of the larger issue in specific areas

Chapter 1
**The History of the Issue**

## Brief History

*1930-1975 Government monopoly on cryptology exists Expense and the scarcity of computing power make the issue unimportant*
*1976-1990 Beginning to go public--public key cryptography arises Costs go down as processing speed goes up 40 bit export limit arises*
*1991-1994 Hardware solutions exist but government controls processes 56 bit and higher export exceptions possible for U S businesses with overseas offices*
*1994-1997 Software solutions emerge as platforms provide faster processing power 128 bit domestic solutions and limited, business only, export exceptions are permitted*

## Administration Efforts 1977-1997

While the arguments being debated last summer have generated much press attention, the issues surrounding the public uses of encryption technology have been causing friction for at least the past 20 years It was the publication of work at Stanford by Whitfield Diffie and Martin Hellman that opened the field of cryptography for academic pursuit absent government funding and for commercial use [12] They developed an algorithm that permitted the efficient transmission of a "public key" safely and then allowed encrypted communication using "private keys "

At about the same time the Diffie-Hellman algorithm[13], was gaining initial attention, the

[12] Susan Landau, et al, Codes, Keys, and Conflicts. Issues in U S. Crypto Policy, Association of Computing Machinery, Inc, June 1994, p 37

[13] see Appendix A. A Cryptology Tutorial

National Bureau of Standards (NBS)[14] was seeking input to a proposal for the development of a Digital Encryption Standard (DES). The government's intent was to provide the banking and financial industries with a secure method of storing and transmitting data These industries were, of course, closely tied to the daily lifeblood of the domestic economy money supply It was a recognition that money supplies could be manipulated, that they were not secure, that led to a more open approach to developing standards at this time Inevitably, however, the involvement of the National Security Agency (NSA) was needed

The NSA had been formed from among several predecessor organizations by Presidential directive in 1952 It maintained a shadowy existence during most of its history Located at Fort Meade, Maryland, employees carried extremely high security clearances The NSA was the premier agency involved in collecting intelligence from across the electronic spectrum during the Cold War Needless to say, they became very good at all things having to do with electronic media It is not surprising, then, that the NSA would be a large part of the government's efforts to standardize DES for domestic use and to restrict its export

Businesses and academics were skeptical that a secretive agency such as NSA could have no ulterior motives when developing commercial standards There were fears about "trapdoors" built into programs that would permit clandestine access There were also cases, with which many academics were familiar, of restraint on publication of sensitive research findings

So a climate of distrust has been present from the outset Unfortunately, each time the government has learned a lesson about dealing with commercial and academic issues, another

[14] Now the National Institute of Standards and Technology (NIST)

bogey appears In 1984, President Reagan issued a directive (NSDD 145/14)[15] demanding stricter controls on the protection of non classified but sensitive information This included encryption related work Once again, business and academics were dismayed to think that some greater motive was lurking behind the front of national security concerns This time, in addition to the usual players, however, the emerging business and companies supporting the personal computer revolution were affected Public outcry was louder and stakeholders were less willing to compromise over unproven national security claims

The Congress stepped in at this time (although they were never particularly far away) by passing the Computer Security Act of 1987 Among its many provisions was the establishment of civilian control over commercial computer issues This had the effect of moving academic and business related encryption work away from NSA purview and into the control of the Department of Commerce's National Institute of Standards and Technology (NIST, formerly NBS)

What followed was a multi year struggle within at least the last two administrations to define what areas of oversight belonged to the Department of Defense, the Department of State, and the Department of Commerce when it came to computer issues At least three times since then a Presidential order has been issued to give Commerce purview over export of commercial encryption products Until November 1996, however, decisions about exports were still being made at the Department of State after approval by DoD (NSA acting as executive for DoD) [16]

Meanwhile, the business and commercial expansion of strong computing power, the

[15] National Security Decision Directive 145/14 established the safeguarding of sensitive but unclassified information that effected national security

[16] See Appendix D

beginnings of the Internet explosion, and the domestic uses of personal computers by a particularly large segment of society led to a greater demand for security products by private, commercial, and other business customers Additionally, the newly acquired ability to communicate worldwide as if it were next door led to the latest clash with government over standardization of domestic products with overseas versions

By 1991, the various forces who today are clashing were almost all taking part along more or less the same issues Except for one group, who had remained out of the arguments up to this point that is the FBI As early as 1986, the FBI realized that electronic advances, particularly computing power would present several challenges to them when investigating crime and developing evidence They initiated a study to examine the potential barriers to electronic evidence collection (wiretaps) that would occur by the spread of encryption technology and by the uses of digital telephone switches Yet getting the FBI to focus on this issue was still difficult

When Senator Joseph Biden introduced Senate Bill S 266, The Comprehensive Counter Terrorist Act, in January 1991, the FBI endorsed the provisions that dealt with encryption controls That bill was withdrawn, but in 1992 the FBI presented a legislative package asking for a wide range of crime prevention and investigation measures that would mitigate the effects of electronic switches in phone systems and restrict the uses of domestic encryption products There were no Senate sponsors for that package

Advances in the science of encryption did not await the resolution of the various groups' differences By late 1991, NIST was proposing a newer encryption standard, Digital Signature Standard (DSS) Again the negative comments during the public response period made clear that old fears and animosities were not resolved

In April 1993, the White House announced the Clipper Chip, a hardware solution to encryption challenges for business and commercial interests, government offices and individual uses It consisted of a sealed silicon chip embedded with a proprietary algorithm developed by NSA (SKIPJACK), a procedure for authorized law enforcement interdiction of message traffic (LEAF), and it featured the DSS [17] A public outcry resulted The media entered the arena of debate, reporting many of the older arguments, awakening the old distrust between government agencies and business concerns, predicting dire consequences for individuals and commercial interests alike Surprisingly, the government was discovered to be still relying on NSA approval[18] for exports of what were supposed to be Commerce Department controlled decisions While that was not directly related to the Clipper program, it was a crisis for an administration that had recently announced and promoted its dedication to the global information superhighway This was perhaps the first policy flop of the current era

Clipper was subjected to intense scrutiny and debate, but was nonetheless approved in February 1994 for use in a variety of devices One fortuitous event to arise from this episode was the suggestion by Vice President Gore to pursue software-based encryption technologies as an alternative to hardware-based approaches Until this time, there was little effort to implement an encryption algorithm in a software application because the calculations were time consuming, the computing power required to make the approach attractive was still somewhat expensive, and the businesses producing encryption devices did not see a market for the method

The failure of Clipper to gain acceptance, however, changed the calculus somewhat Also,

[17] see Glossary

[18] NSA was supposed to offer advice when consulted, not vote approval or disapproval

around this time both the Pentium chip for PCs and wider access to the Internet provided market researchers a fresh perspective on the potential for software-based encryption products to be developed and sold By 1995, a slew of new products and improved older ones were flooding the domestic market But the realization by software manufacturers that control of foreign markets was not guaranteed because of export restrictions led to the next round of debate

In November 1995, the administration proposed a still newer standard, the Escrowed Encryption Standard (EES) As they had with those standards before it, the business and academic community challenged the government's approach to developing a proprietary algorithm This time, however, the specter of mandatory key recovery was introduced Even a voluntary key escrow system was not acceptable to the large constituency that feared government access to private records and government market control

When the administration tried a conciliatory effort in July 1996 with the publication of its Statement on Commercial Encryption Policy[19], a discussion that attempted to justify key escrow, the non government interests involved in the debate finally revolted Several months earlier, in May, the National Research Council had published a report[20] recommending in part, that the government should back away from imposing standards and permit the market to determine the outcome of encryption technology, including exportation of products This was anathema to the FBI and to at least a significant number of leaders within the NSA The administration appeared to be deaf to the interests of the business and commercial community although to their credit,

[19] Appendix C Statement on Commercial Encryption Policy

[20] Cryptology's Role in Securing the Information Society, National Research Council Committee to Study Cryptology Policy, U S GPO, May 1996

many key members of the NSA and DoD were struggling with the issue Worse, it appeared to be uncaring about the privacy concerns of individuals, at least based on the perceptions of those outside the process

By the time the President published his Framework for Global Electronic Commerce,[21] in July 1997, which repudiated domestic taxes on electronic media and offered many more conciliatory efforts, the stakeholders were no longer willing to accept the administration's proposals at face value Congress had gained the attention of the major players with a variety of bills competing to regulate and define the competing interests that were never satisfied by the administration's efforts

**Legislative Solutions**

Congress had not been idle during the previous 20 years by any means As early as 1978, they tasked the GAO with conducting a study to determine if the administration was taking appropriate steps to address computing issues, including encryption policy Again in 1985, the GAO reviewed the procedures that resulted in the DES standard Both times, the conclusion was that the administration was acting properly

But by 1987, with the passage of the Computer Security Act[22], it was clear that Congress intended for domestic, private, and commercial electronic enterprises to be administered separately from national security issues They were especially keen to get NSA out of the business of controlling decisions about computer developments by U S businesses

---

[21] William J Clinton and Albert Gore, A Framework for Global Electronic Commerce, U S GPO, July 1, 1997, see Appendix B

[22] The Computer Security Act of 1987, Congress of the United States, U S GPO

In 1991 and 1992, the Congress was content to wait and see what developed as the administration prepared its Clipper proposal, of which they were well aware Bills introduced in both the House and the Senate addressing dual use restrictions and controls were quietly dropped The FBI request for enabling legislation to control digital telephony was ignored In 1993, another GAO report reviewed government actions and stakeholder arguments since 1973 [23] It provided the basis for Congressional action as the Clipper program foundered

In May 1994 the Digital Telephony Act was introduced It provided means for law enforcement to pursue electronic surveillance within digital networks, requiring manufacturers to build access into the system It was signed into law in October 1994[24] During 1996, several bills in the Senate and one in the House were introduced addressing a variety of computer related issues that Congress had watched maturing for the past several years None of these was pushed forward, however, and each died a quiet death before that session ended

In1997 a variety of new legislative attempts in the House and Senate emerged Each was based on the previous year's aborted bills These are summarized below

**Legislative Actions During 1997**

The most talked about and robust bill introduced this Congress, the **Security and Freedom through Encryption (SAFE) Act**, H R 695, was sponsored by Representatives Goodlatte and Eshoo and has more than 250 cosponsors SAFE was unanimously approved by the House

[23] Richard C Stiener, Communications Privacy- Federal Policy and Actions, U S GAO, November 8, 1993

[24] Actually called the Computer Assistance to Law Enforcement Act of 1994, Congress of the United States, U S GPO, October 1994 In April 1998, the FCC stated that the FBI was abusing its power as executive implementing agent of CALEA, demanding greater access than the Act requires

Judiciary Committee on May 14, 1997 On July 22, it was approved by the House International Relations Committee by a voice vote On September 9, 1997, the House National Security Committee added an amendment and approved the amended bill On September 11, 1997, the House Permanent Select Committee on Intelligence added an amendment and passed it On September 24, 1997, the House Commerce Committee added an amendment that changed the bill by calling for the creation of a National Electronic Technologies Center that would assist law enforcement in research and would provide assistance to federal, state, and local law enforcement agencies in coping with encryption encountered in the course of investigations The amendment also would direct the National Telecommunications and Information Administration (NTIA) to conduct a study of the implications of mandatory key recovery, and increases the criminal penalties under SAFE for the use of encryption in the furtherance of a federal felony The bill was never scheduled for a floor vote and died with the 104th Congress

**The Computer Security Enhancement Act of 1997, H.R. 1903**, was introduced by Representative Sensenbrenner on June 17, 1997 It would amend and update the National Institute of Standards and Technology Act to (1) upon request from the private sector, assist in establishing voluntary interoperable standards, guidelines, and associated methods and techniques to facilitate and expedite the establishment of non-Federal public key management infrastructures that can be used to communicate with and conduct transactions with the Federal Government, and (2) provide assistance to Federal agencies in the protection of computer networks, and coordinate Federal response efforts related to unauthorized access to Federal computer systems The bill also would authorize NIST to perform evaluation and tests of (1) information technologies to assess security vulnerabilities, and (2) commercially available security products for their suitability

for use by Federal agencies for protecting sensitive information in computer systems This bill was passed by the House on September 16, 1997, and was referred to the Senate Committee on Commerce, where it awaits consideration

**The Communications Privacy and Consumer Empowerment Act** was introduced by Representative Markey on June 19, 1997 This bill would codify existing domestic use policy, permitting unrestricted use of any encryption It would also prohibit the government from requiring key recovery as a criterion for encryption licensing The bill was referred to the House Committee on Commerce

**The Encrypted Communications Privacy Act (ECPA II), S. 376**, was introduced by Senator Leahy on February 27, 1997 ECPA II would prohibit mandatory use of key recovery but would permit law enforcement to obtain keys if recovery were used It would also make it a crime to use cryptography to obstruct justice The bill was referred to the Senate Judiciary Committee, which held hearings on it on July 9, 1997

**The Promotion of Commerce Online in the Digital Era (Pro-CODE) Act, S. 377** was introduced by Senator Burns on February 27, 1997 Pro-CODE was considered one of the most privacy friendly encryption bills Pro-CODE would have expanded the protections against government intrusion rather than enhancing wiretap authority The Secure Public Networks Act was substituted for Pro-CODE when it came for a vote in the Senate Commerce committee on March 19, 1997

**Secure Public Networks Act (SPN), S. 909** is the Clinton Administration's bill It was sponsored by Senators McCain and Kerrey It requires third-parties holding decryption keys to surrender them in response to a subpoena without notice to the encryption user While its

sponsors claim that it would not make key recovery mandatory, SPN would require the use of key recovery systems in order to obtain the "public key certificates" needed to participate in electronic commerce and would require key recovery for all secure networks built with any federal funds -- including the Internet II project and most university networks It creates new federal crimes dealing with the use of encryption and key recovery SPN directs the President to negotiate with foreign countries to create a worldwide system for international government access to escrowed keys The bill was referred to the Senate Commerce Committee in March

Why Congress Acted

There are several versions of an explanation about why Congress waited until 1996 before approaching this problem It was clear following the 1987 Computer Security Act that subsequent administrations (Reagan, Bush, Clinton) were struggling with electronic issues and handling them badly Chapter 2 will analyze this question more fully, but for now three explanations might suffice These are not mutually exclusive by any means

-Administration request for enabling legislation to pursue current policy It is not surprising to think that the Clinton Administration would wait as long as possible, in the face of a Republican-controlled Congress, before asking for help in its attempt to set policy The Secure Public Networks Act reflects this approach

-business lobby pressure to define export limitations in law rather than in policy Clearly, by 1996, business was at wits end trying to cope with the administration It is equally likely that the business lobby was effective in pushing for at least two of the bills before the current session of Congress, the SAFE bill and the Pro-CODE bill

-Congressional timing and interest It has been the prerogative of the Congress to permit

certain issues to mature before addressing them This seems to be the case for much of the absence of legislation between 1987 and 1996 Certainly, in each of the preceding sessions, some more pressing matter demanded Congressional focus anyway

## Judicial Review

Encryption Cases Decided In the Courts

There have been three legal challenges mounted against the export controls on encryption technology While decisions in these cases have not been made final, both Congress and the administration are aware of the judicial temper as it is manifest by this issue Two of the cases, Junger v U S Department of Commerce and Karn v U S Department of State, are still in argument at the trial level In the third case, Bernstein v U S Department of State, the trial court has found that the export control laws restricting encryption are an unconstitutional prior restraint on speech

The Facts

Daniel J Bernstein was a Ph D student in Mathematics at the University of California at Berkeley He wrote an encryption program, Snuffle[25], along with a document describing the program, that he wanted to post on the Internet for discussion and scrutiny by other cryptographers After asking the State Department, Mr Bernstein was informed that he would need a license to be an arms dealer before he could post his encryption algorithm and descriptive document to the net Further, if he applied for a license his request would be denied because his algorithm was too secure Mr Bernstein sued His attorneys claimed that the export controls act as a prior restraint on his constitutionally protected speech and are over broad to serve their

[25] Daniel Berstein, Snuffle, a computer source code, (under research)

purpose of protecting national security This case was filed in the Federal District Court for the Northern District of California and was heard by Judge Marilyn Hall Patel

Court's Ruling

Judge Patel has made several rulings in this case The first ruling (Bernstein I, 922 F Supp 1426 (N D Cal 1996)) was on April 15, 1996, and was in response to the government's motion to dismiss the case for lack of jurisdiction The court held that source code was speech protected by the First Amendment, and the court therefore had jurisdiction in the case

The second ruling (Bernstein II, 945 F Supp 1279 (N D Cal 1996)) was on December 6, 1996, and responded to( now) Dr Bernstein's motion for an injunction so he could post materials to a Web site for students in his cryptography course The court held that Bernstein could publish for his class while the rest of the case was being decided

The final ruling (Bernstein III) was on August 25, 1997, when the court held that the restrictions against the publication on encryption were an unconstitutional prior restraint on speech

Post Facto Actions

The court granted an injunction to Professor Bernstein, forbidding the government from prosecuting him for exporting the encryption program he wrote, or any other encryption programs The court specifically stated that it considered granting an injunction against the enforcement of any encryption restrictions The court declined to do this, however, stating that it expected an appeal and wanted the most narrow holding it could devise The court also held that allowing printed source code to be exported undermined the government's claim that this export control scheme protects any national security interest The court opined that distinguishing

printed from electronic matter probably violates the First Amendment under Reno v ACLU (1997), which held that Internet speech deserves the same protections as printed speech

In December the US 9th Circuit Court of Appeals heard government arguments attempting to set Judge Patel's ruling aside The public questioning of the government's lawyers indicated that the Appeals Court was cognizant of the relevant issues and tended to favor individual privacy over government export restrictions [26]

**Outlook and Outcomes--1998 and Beyond**

The status of the encryption technology control issues at the end of 1997 was mixed The government insists on control either through proprietary algorithms or key escrow encryption systems There is no movement toward a compromise that would permit greater freedom to export strong encryption products Congress did not pass any of the competing bills before the 104th session It will await another cycle of legislative debate before action occurs from that area It will be 1999 or later before a significant case comes before the Supreme Court Meanwhile, District Court cases will shape legal precedent in a variety of ways without impacting the problem significantly The 9th Circuit appeal will not end until a ruling on the issues is forthcoming sometime in the spring of 1998 Without a second case from another Circuit, however, it is unlikely that this issue will get a fast track docket from the Supreme Court in 1998

Business is coping with the impact of marketing strong encryption domestically while selling weaker products abroad Whether this will ultimately harm market shares remains to be seen The United Kingdom, Germany, and France(among others) are moving forward with competing

[26] The 9th Circuit is, however, the most overturned court when Supreme Court reviews hear cases arising from there In the past 10 years 26 of 28 9th Circuit decisions have been overturned

products to fill the void left by an international absence of U S products Each of these countries impose sharper export restrictions on their companies' products than do U S rules, but markets within these countries are less open to U S products themselves Global dependence on U S software, however, hinders the use of substitute products

One Commerce Department official has pointed out that other countries are relying on U S restrictions to keep strong encryption away from their people Absent a U S controlled export regime, countries such as France may well impose even stricter standards against the importing of U S products Meanwhile, business with overseas offices are being granted limited export permission under the current rules This is being conducted on a case by case basis only and can stop at any time

There are no cases now where the FBI has been prevented from investigating a crime or prosecuting a suspect for the lack of decrypted data Director Freeh, in his testimony to Congressional committees this past summer, selectively provided examples of potential limits to FBI evidence development if encryption becomes widespread His examples have, however, been shown by Dorothy Denning at Georgetown University, to be overstated[27] Similarly, there are no cases in which the ability to apply key escrowed decryption would have prevented a crime from occurring

Finally, no individual has been forced into needlessly losing his privacy over an issue of encryption availability Nor has the government pursued innocent persons via wiretap and electronic surveillance by exploiting weaknesses in cryptologic products

[27] Dorothy Denning, Encryption Technology and Crime, Searching for a Neutral Zone, Educomm Review, September/October 1997, p 39

In January 1998, a security conference sponsored by RSA, Inc invited government and business participants to San Francisco to discuss encryption issues facing the industry and government, both domestically and internationally The sponsors hoped to frame the encryption control debate in such a way that Congressional actions in the 1998 session will be influenced Speakers included Vice President Al Gore, Presidential domestic advisor, Ira Magaziner, and representatives from the NSA and the FBI as well as industry advocates for less restrictive encryption technology control

It is likely that 1998 will see a reintroduction of the SAFE bill in the House With strong support among members it should emerge from the Rules Committee in a version very similar to the original, that is to say, without the domestic controls introduced in the Judiciary Committee The 9th Circuit appeal of the Bernstein case will issue an opinion in March or April If the court affirms Judge Patel's ruling the Department of Justice will seek a Supreme Court hearing on the issues That is unlikely to be granted until at least one other review court has ruled on similar issues Ira Magaziner has stated that the administration will wait for the issues to mature before directing specific policy changes for export controls or other encryption technology controls

Meanwhile, special interest groups for privacy matters, businesses, academics, and the press have maintained an educational campaign aimed at clarifying the privacy and free market issues involved They have also attacked the FBI's record of abuse in historic wiretap cases (see Diffie-Landau) to show that increasing the reach of law enforcement into decryption capability is dangerous for civil liberties They can be expected to continue this approach

SPRING 1998 UPDATES (as of April 1998)

Members of Congress resubmitted two bills that would change the existing export controls for encryption products The first is an identical version of the original Goodlatte bill in the House while the other is a repeated version of the administration's bill in the Senate Neither bill is progressing Since this is an election year, this issue will likely remain out of the scheduled sessions Rather, committee work is expected to move the actions along at a pace that maintains the debate without threatening to upset more important legislation in this session

Ira Magaziner, the White House policy spokesman for encryption related matters, agrees with both industry and privacy advocates that current administration policy needs revision In remarks earlier this year, he stated that the electronic commerce policy statement of November 1996 underestimated the resistance to key recovery schemes proposed by the administration He acknowledged that the Department of Justice and the Department of Commerce were not providing a coordinated position His goal is to continue to permit the debate within the administration to develop while seeking areas where compromises with business and privacy advocates can be obtained

Commerce Secretary William Daley, the cabinet secretary responsible for implementing US encryption export control policy, says "our implementation has been a failure" In remarks in March 1998, the Secretary stated that the application of the original rules was poorly done Once the rules were liberalized, in November 1996, giving more discretionary power to the Department of Commerce and less to the Department of State, the process never was fully streamlined The result was that some companies were granted exemptions to the 56 bit key length restrictions while others were not Additionally, the length of time taken to process requests for export licenses remained longer than reasonable for business applicants He did not propose any

solutions, however, rather stating that the department would await congressional clarification of the law

In April 1998, the FCC released a report indicating that the FBI is abusing its wiretap authority under both the 1976 Omnibus Crime Control Act and the 1994 CALEA The FCC investigation responded to industry complaints that the FBI, as the implementing agency of the 1994 CALEA, was adding restrictive provisions to the planned accessibility features of digital switched networks These regulations go beyond the mandate the Act provides, states an FCC spokesman There has been no FBI response

Two companies, RSA and Network Associates, announced that they have legally circumvented encryption export rules Each states that a foreign business partner will be able to offer a product compatible with their domestic encryption software In the case of RSA, the export of written source code permitted a software product to be developed overseas In the Network Associates case, a partnership with a Dutch firm enabled them to prepare a comparable product The Commerce Department stated it would examine whether any U S laws were violated in these cases Experts agree, however, that both companies appear to be operating within the strict provisions of the U S law

The source code of newly marketed digital phones was cracked by a team of university researchers in early April They were able to examine the code, discover the encryption algorithm, and provide the decryption keys after several days of laboratory effort This shows that source code can enhance brute force means to decrypt longer key lengths (the digital phone used either a 56 bit or a 64 bit key) Officials pointed out, however, that the team had access to the equipment and a powerful lab in which to exploit it without interruption "This is not the same as someone

off the street gaining access to encrypted conversations", stated one industry official

An NSA paper, Threat and Vulnerability Model for Key Recovery, shows that when the keys to encrypted data are made accessible to law enforcement through a third party the risk that a key may be stolen or compromised in some way rises significantly The NSA paper, dated February 18, outlines nearly 20 additional attacks and vulnerabilities Taken as a whole, these attacks make it clear that key recovery will be a risky and costly proposition for most computer users This position underlies the fear among privacy and business advocates that government mandated key recovery schemes are an infringement of protected liberties

## Chapter 2.
## Analysis

### The Stakeholders' Views

There are four groups with a stake in the outcome of the encryption control debate These are individuals, businesses, academia, and government A potential fifth stakeholder is represented generally by foreign interests Yet within each of these groups there are by no means a uniform set of interests

#### Individuals

Individuals may be subdivided into four other broad groups of interests First, are those persons who prize privacy, anonymity, and the freedom to be left alone They resent any intrusion by anyone into the areas they choose to define as off limits Issues for this group revolve around a notion of inalienable rights to privacy, whether constitutionally defined or not They seek not only the ability to encode and decode at will, without any government intervention, but also the protection from snooping by both government and business The former through any means of regulation, restriction, or information gathering and the latter through over use of personal data obtained in e-commerce or other Internet related activities

Second there are individuals who simply wish to conduct e-commerce with at least the degree of trust and protection available in other, non electronic transactions Privacy is less of an issue to these people than is safety from those who steal credit information or who defraud shoppers They recognize encryption technology as a new tool to protect them in the field of electronic

banking, credit purchases, and information gathering research on the Net

The third group probably contains the greatest number of individuals That is the vast majority who are unconcerned, unaware, or uninterested in the debate They may or may not be using the Internet, e-mail, e-commerce, or other electronic transactions The fact that electronic databases are mined for personal information is a fact of life The presence of government regulations is expected The need for privacy is not a high priority for them They are Richard Nixon's great "Silent Majority" It is this group that is targeted by both privacy advocates, business interests and government officials in an attempt to gain a public opinion surge sufficient to sway the policy outcome

Arguably, a fourth group emerges from the realm of the individual interest That is the criminal, be he credit thief, pedophile, or terrorist Obviously, this set of individuals benefits from the least restrictive encryption controls which will permit them to pursue their nefarious ways to exploit the public, while hidden from view Equally obviously, this group is quiet in the debate

Whatever form the interests of individuals take, they are represented vocally in the debate by a variety of special interest groups These groups include the Electronic Freedom Foundation and the American Civil Liberties Union, among others Individuals are also well represented by the courts Even when a majority might rule against an individual privacy issue, a strong dissenting opinion is possible and can do good Justice Brandeis' famous dissent in Griswald v U S is credited with establishing the right to freedom from government wiretap without a warrant although the majority court opinion went the other way [28]

**Business**

[28] Griswald v U S , U S Supreme Court, 1928

Business concerns fall into two broad categories and further subdivide into many other interests The primary concern of businesses in the encryption control debate is the freedom to develop markets, both domestically and abroad They wish to sell a set of hardware and software products for use by consumers An equally important view is to obtain the means to protect competitive secrets, trade data, financial data, and other business information from misuse or disclosure while either in storage or in transit

Both software developers and hardware makers agree that the means to market encryption products and devices are now plainly in the private sector after years of being a government controlled enterprise Businesses are anxious to freely exploit this emerging market Economies of scale, however, are better served when the variety of products offered can inter-operate and provide similar levels of service to all customers This becomes the crux of the business interest for free exporting of encryption products as capable as those provided domestically Indeed, having captured the domestic market through years of saturation sales and upgrades to products, the manufacturers now wish to secure overseas sales of the same products with the same success and in the face of renewed assaults against domestic uses of encryption, to preserve the market they have established at home

Commercial interests are also concerned that the security of electronic commerce transactions depends on continuously developing and upgrading a family of related encryption technologies that improve transaction speed, insure non repudiation of sales, promote authenticity determinations and guarantee inter-operability of products across a suite of other enabling software technologies such as JAVA scripts and applets, electronic forms, and electronic delivery systems

Banks are among the leaders of this viewpoint Their transactions occur daily in staggering amounts of data volume and currency value The global economic interaction of commerce demands that banks share data across national boundaries with the highest degree of security Customers, of course, will accept nothing less than absolute accuracy and safety in currency transactions

Telecommunications companies are a second example of commercial business interests heavily influenced by the international availability of strong encryption As the backbone of the Internet and such incarnations as the Virtual Private Network (VPN) in which businesses conduct internal matters over the public network, telecommunications companies recognize the need for a protected environment that speeds legitimate transactions while guarding against intrusion or abuse

**Academia**

Sharing research and development with colleagues, conducting a dialogue with fellow researchers, and broadly publishing results of effort by academics is fundamental to the traditions of advanced studies by professionals Just as the economy has gone global, so has the ability to conduct academic study among a worldwide audience Thus, academia represents an additional group of special interests

The needs expressed by academics haven't changed in the years that cryptology has been studied as a professional field They seek unencumbered publication, without restraint of their research findings They seek the ability to share their knowledge in private exchanges as well as teacher-student relationships The Internet promotes this activity globally There is a global classroom as well as a virtual laboratory possible today that increases the opportunities for

exchange and advancement of knowledge

The government's propensity for prior restraint and restriction of research in the field of cryptology is not as onerous today as it was as recently as the 1980's, but it still exists to a degree that researchers find restrictive The cases of Phil Zimmerman or Daniel Bernstein illustrate this

As a group, academics are much smaller than the other private interests taking part in the encryption control debate, but no less important Generally, they have lent their weight to the efforts of special interest organizations to promote both individual freedoms and business interests It is clear that academics are involved much more in business practices today than in the past Much early work in software development follows from these closer relationships between academia and business

The vocal part of both business and academic interests is advanced by a variety of groups similar to those promoting individual privacy These include the Electronic Frontier Foundation, the Software Business Alliance, the Internet Privacy Coalition, and the Cryptology Project, among others [29]

**Government**

Each of the three branches of the federal government (and by extension the corresponding portions of state governments) has a role and a series of interests in shaping and developing the encryption technology policies of the United States Unfortunately, the variety of interests collides quite often

Administration Interests

The Executive Office of the President (EOP) has stated clearly its commitment to electronic

[29] See appendix C, Sources Consulted for the Home page URL of these groups

commerce and the enhancement of the National Information Infrastructure (NII) as a part of the Global Information Infrastructure (GII) The Information Infrastructure Task Force (IITF) under the titular direction of the vice-president has undertaken the effort to define and direct administration policies and support to a variety of undertakings related to the explosion of digital computing, electronic communications, the Internet, and electronic commerce Ira Magaziner, the President's at-large domestic policy advisor, has become the Field Marshal of the executive branch in establishing broad direction to promote and exploit U S dominance in this area Generally, the policy direction is to promote unfettered, market driven development of products and services while guarding against unfair business practices, exploitation of the public, and predatory trust actions This is not consistent with the Secure Public Networks proposal supported by the administration in the Senate That bill promotes key recovery schemes to protect law enforcement and national security interests in addition to the stated policy aims of the administration

The President's Commission on Critical Infrastructure Protection (PCCIP) also represents a range of issues regarding this area Its report in November 1997 identified broad areas where Information Warfare attacks against the installed base of electronically controlled utility, transportation, data storage, and financial infrastructures required government involvement to prevent a loss of function among these areas Regarding encryption, the commission supported the current policy to restrict exports while promoting domestic uses and sponsoring key recovery programs

The Commerce Department has responsibility for export controls and business support Commerce performs its tasks with due regard to the existing law, regulations, and policy guidance

provided by other parts of government While it has become the target of the special interest groups because of their role in restricting export of strong encryption, its role is more functional than influential The Commerce Department can assume a more active role in recommending policies that promote business interests or that restrict trade, but for now it has avoided that role In current cases, however, Commerce has sponsored a degree of loosening of the ITAR restrictions against 56 bit and 128 bit export licenses for businesses with overseas offices and banking interests It remains an active part of the overall administration effort to find a cohesive policy

The National Institute of Standards and Technology (NIST) (another Department of Commerce activity) is directly responsible for developing and promoting the commercial and domestic uses of encryption technology under the Computer Security Act of 1987 It is, however, underfunded, under skilled, and under manned to carry out this task without the direct involvement of the NSA While this is viewed by many as a clear violation of the 1987 CSA, it is also impractical to take another approach under current funding restraints Nonetheless, NIST is finding its own voice in the debate over controls and future developments

The Department of Defense and the Department of State share responsibility for the control of national security information and for the exploitation of foreign information obtained by any means It is clear that within the administration and under the authority of the National Security Act of 1947 this role grants them a broad interest in the uses and capability of encryption and decryption tools Through the NSA, this role is carried out What has changed is the degree to which the government monopoly is eroded Business and individuals now have access to tools that until very recently were impractical to obtain The challenges this presents can be represented

by two views Both a conservative view that the NSA's traditional purview should remain intact and a progressive view that new opportunities and adjustments to the fulfillment of the national security mission are necessary Either way, NSA remains an important stakeholder in this debate

The Justice Department and, more importantly, the FBI have expanded their roles in this area to address new forms of crime as well as new ways that traditional law breaking occurs Encryption presents the law enforcement community with a serious challenge that is larger in scope than that faced by the NSA and more serious in the potential for failure in its effects on the citizens of the United States This is so because the threats to public safety from the criminal uses of encryption are more numerous than threats to national security from hostile foreign governments Clearly the FBI role in defining and recommending policy with regard to encryption uses is valid The terrorist threat alone mandates a strong federal law enforcement program to identify, prevent, investigate, and punish criminal behavior Other criminal activities including crimes against children, business exploitation of consumers, drug related crime, and securities fraud might represent greater challenges to prevention and investigation measures when encryption is available This is what the FBI believes

Congressional Interests

The Congress continues to fulfill its role as the deliberative body that examines issues carefully and ultimately establishes law to control the interactions of various interests and the government In the case of encryption control, the process has been as cumbersome and messy as the Constitutional Framers envisioned

In its broadest sense, the Congress seeks to limit government intrusion into private and commercial transactions while at the same time providing a leveling force, through legislative

action, that promotes a variety of interests In the case of encryption controls, this follows from a legislative history of first promoting commerce, second, protecting individual freedoms, third protecting national security, and fourth providing tools to law enforcement The role played by Congress is critical, especially when policy making in the executive branch becomes contradictory

The existing law that bears on the case of encryption includes the original Constitutional restrictions of export tariffs, the Bill of Rights for protection of individual freedom, the National Security Act of 1947, the Omnibus Crime Control Act of 1968 (which restricts wiretap authority), the Computer Security Act of 1987, the Digital Telephony Act of 1994[30], and the variety of bills now in the Congress for the promotion or restriction of encryption technologies

Court Interests

The federal court system maintains its role as the final arbiter of conflicting interests In the case of encryption control, some defining issues have surfaced at the Appeals Court level and will probably come before the Supreme Court in 1999 There is a mixed history of lower court and Supreme Court rulings that bear on the issue

---

Generally, the courts favor national security issues over all others They seldom challenge legitimate claims by government that bear on this Spurious claims of protection for national security are, however, often rejected The record of favoring law enforcement over private or business interests is mixed Through the 19th century and well into the 1960's court rulings tended to restrict police practices while protecting Constitutional rights against police searches, and for unfettered speech Since the 1970's the courts have more often supported law enforcement claims

---

[30] Actually by this time it was called the Communications Assistance for Law Enforcement Act (CALEA) It both granted new powers and restricted older abuses of law enforcement in the area of electronic surveillance of which wiretap is a subset

for the public safety over individual rights This change is not absolute since many cases are still decided in favor of individual freedoms The outcome in the encryption issue will depend both on the type of case brought before the court (free speech, freedom from search, privacy, or self incrimination) and on the nature of the crime which originally generates the hearing [31]

## Foreign Interests

Foreign interests fall into two very broad categories The first includes the actions and policies of other governments The second includes the needs and rights of business or individuals within those foreign countries

### Governments

Among foreign governments there seems to be a period of waiting to see what the United States does Among the European and other western style democracies there are differing degrees of individual rights and government controls which are traditionally applied Countries such as Australia and New Zealand tend to be more supportive of business rights than individual ones yet will often promote stricter law enforcement regimes than the United States does The United Kingdom favors government somewhat more than individuals or businesses France is generally more restrictive of individual rights, more liberal toward business rights and more supportive of intrusive law enforcement Germany, Belgium, the Netherlands, the Scandinavian countries, and the emerging Eastern Europeans tend to promote individual rights while restricting law

[31] It is ironic that many cases that seek to define a protection of rights over police powers have the unfortunate aspect that the accused whose rights are alleged to be violated is in fact a bona fide criminal and the proximate cause of his original conviction is a heinous crime of one type or another

enforcement Totalitarian governments and most developing nations as well as most Asian cultures subordinate the individual to the state in almost all cases [32]

Foreign Users (Business and Individuals)

The United States enjoys a 95% share of the international software development and distribution market This advantage means that most foreign users require the U S version of encryption software to inter-operate in the global market While foreign businesses, especially those in Germany, France, and the United Kingdom, are developing their own products, these are of limited utility against an installed base of U S applications such as Microsoft Office 97, Corel Suite 8, Lotus Smart suite, and other databases, accounting packages, and accessory programs (including browsers and e-mail) Foreign users, therefore depend on the availability of U S exported encryption products [33]

**Summary**

In all there are perhaps 21 unique groups that stand to benefit or suffer from the outcome of the encryption technology control debate and its subsequent policy formulation Each has a set of interests that often coincide and sometimes conflict with the interests of other groups Many are represented by the same or similar lobbying bodies as the issue is debated in Congress and among the administration's various agencies

Simplicity in framing the analysis of each group's views and needs suggests that the following

---

[32] CRYPTOGRAPHY AND LIBERTY AN INTERNATIONAL SURVEY OF ENCRYPTION POLICY, The Global Internet Liberty Campaign, http //www gilc org, January 1998

[33] Eric Wilson, Impossible to Administer in Borderless Commerce, Australian Financial Times, January 22, 1998

framework will be useful in the remainder of this chapter The nexus of the debate pits individuals ( including academics) and business on one side (favoring the least restrictive policies) against the executive branch agencies for national security and law enforcement on the other The Executive Office of the President, the Congress, and the Courts represent more moderate views Foreign interests, both government and private, are of secondary involvement

It might be even more useful to reduce the stakeholder arguments to a contest between only two groups citizens, consisting of both individual and corporate persons versus law enforcement This last approach gets right to the heart of the matter since the NSA has taken a very quiet role since the fall of 1997 It has been FBI Director Louis Freeh who is carrying the administration's burden of argument to establish key recovery systems as the only legal form of encryption permitted

In the meanwhile, however, an analysis of the arguments of the broader group is still in order

## Stakeholder Analysis

### Individual Privacy Concerns

Constitutional protections and the intent of the Framers show a clear bias in favor of individual protection from the intrusions of government The minutes of the Constitutional Convention as well as the final text of the Constitution and also the Federalist papers establish that the purpose of the government is to protect citizens from all hazards including overbearing government policies This is the foundation upon which privacy advocates base their claims for the availability of open and unfettered encryption technology

The preamble to the Constitution states among its purposes, "[to] secure the blessings of liberty " as a goal The Bill of Rights, which was debated as a part of the main body and subsequently added to the Constitution within several years, provides enumerated rights favoring free speech and assembly (I), protecting against government searches, seizure (IV and V), and arrest without warrant (V), protection from self incrimination (V), and protection from anonymous incrimination (VI) It also provides that rights not enumerated still exist and are protected (IX)

As pertains to the possession, use, and distribution of encryption technologies the 4th and 5th Amendment proscriptions against searches, seizure, and incrimination are probably the strongest support to the individual Inasmuch as any law restricts the use of encrypted matter and thus prevents a citizen from enjoying freedom from government intrusion, it is probably a violation of these amendments

A Justice of the Supreme Court once provided an allegory about the nature of privacy which I will paraphrase here On its face, the use of encryption is no different from the use of a front door

When it is open, it invites those outside to peer within But once it is shut, it prevents those outside from any certain knowledge of what is within

The courts have defined and defended this principle in a variety of rulings over the years The words of Justice Louis Brandeis perhaps carry the meaning most succinctly

> *"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection [And now] the right to life has come to mean the right to enjoy life — the right to be left alone.*
>
> *When the Fourth and Fifth Amendments were adopted the form that evil had heretofore taken had been necessarily simple Force and violence were then the only means known to man by which a government could directly impel self-incrimination [But] time works changes, brings into existence new conditions and purposes Subtler and more far reaching means of invading privacy have become available to the government Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.*
>
> *The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness They recognized the significance of man's spiritual nature, of his feelings, and his intellect. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations They conferred, as against the government, the right to be left alone — the most comprehensive of rights and the right most valued by civilized man To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment And the use of evidence in a criminal proceeding of facts ascertained by such intrusion be deemed a violation of the Fifth "* (Brandeis, 1928, Olmsted v U S pp 473, 477-478)

The record of the Supreme Court is mixed nonetheless In Olmsted v U S it ruled in favor of broad police powers The Court reversed this in Griswold v U S several years later Since the 1980's a conservative court has tended to favor government, particularly in the matter of anti crime measures

Michael Froomkin, a Professor of Law at the University of Miami, has conducted an extensive study of the encryption issue and the body of law and judicial rulings that impact the current policy debate [34] He concludes that "assaults" upon individual rights have increased since Justice Brandeis' 1928 comments The weight of modern rulings, particularly when national security is cited as justification, falls against the individual In the encryption debate he foresees a closely argued opinion eventually emerging from the Supreme Court that compromises individual freedoms in favor of narrowly defined government interests for national security and law enforcement

While this may be a just and fair ruling, when it happens, it will not mitigate the lack of trust civil libertarians feel when government assumes control of new technologies or carves new areas of involvement in personal lives

Frank Fukuyama, in his book Trust The Social Virtues and the Creation of Prosperity[35], discusses the concept that society functions within a circle of trusted relationships When trust exists, day to day functions occur smoothly Once violated, however, the trust is difficult to replace and day to day operations become rough and inconsistent One of the keys to this concept is the notion that transactions maintain transparency to those involved Trust is built upon the idea that what one can see operating fairly, justly, or openly can also proceed smoothly Without transparency, however, trust withers [36]

[34] Michael Froomkin, The Metaphor is the Key, op cit , p

[35] Frank Fukuyama, Trust The Social Virtues and the Creation of Prosperity, p 8-11

[36] Ibid, p 22-24

Whitfield Diffie and Susan Landau, authors of Privacy on the Line[37] agree They discuss the loss of transparency in communication which arises from electronic means replacing face to face methods of discourse as well as the undetectability of eavesdropping (wiretapping) by governments (or others) upon private conversations (or transactions) Diffie and Landau argue that encryption restores such transparency and rebuilds trusted systems This is not possible, however, if key recovery schemes exist [38]

It is also noteworthy, that while citizens expect a certain amount of intrusion into their lives, in the name of public safety, they will not tolerate abuses of that privilege Yet opening the door to guaranteed decryption of their messages "feels" overly intrusive

Wiretapping and search rules applied since World War II have already opened the door to the kind of intrusions contemplated by key recovery schemes Following a series of Presidential findings from Roosevelt to Johnson that became increasingly intrusive and uncontrolled, the Congress enacted the Omnibus Crime Control and Safe Streets Act in 1968 This permitted defined uses of electronic surveillance including wiretap within strict guidelines but also proscribed many potential abuses Congress followed this with the Foreign Intelligence Surveillance Act (FISA) in 1978 as a result of the Church Committee hearings into abuses of the CIA in domestic operations Unfortunately, in addition to granting specific powers to counter intelligence officers pursuing national security protection issues, the FISA granted broad surveillance powers to federal police for pursuing domestic crime if it could be shown that

[37] Whitfield Diffie and Susan Landau, Privacy on the Line, The Politics of Wiretapping and Encryption, MIT Press, January 1998

[38] Ibid

national security matters were involved Not surprisingly, most wiretaps are now for that purpose, including drug-related and organized crime related investigations [39]

Again, while Americans in the great majority are willing to accept many of these intrusions, they eschew the corresponding abuses They accept the concept that threats, both foreign and domestic, exist and that tools to fight these threats might require a collective sacrifice of some degree of freedom They do not accept abuses, however, regardless of the intent of the abuser A discussion of the FBI record of surveillance abuse follows in a future section[40], but suffice it to say, the concept of trust is eroded as numerous cases give rise to what is perhaps citizens' worst fear That is that once one's privacy is violated, once a protected communication is compromised, the nature of personal privacy cannot be repaired or redressed

All this does not really cover the entire issue There are some effective arguments that restrict one's right to privacy as well The world has indeed grown complicated and individuals face a myriad of choices as to how they operate within this complexity Although people often do not view it this way, there are voluntary choices that Americans make every day that open the "front door" into their private world

Credit card transactions, health care transactions, employment, government benefit eligibility, and a host of similar things require the exchange of information in order to avail oneself of a convenient service Some of these may be candidates for government regulation, such as the use

[39] Diffie, Landau, op cit

[40] See "Stakeholder Analysis sub section on Law Enforcement The Church Commission disclosed that illegal and overly broad wiretap and electronic surveillance was rampant in the Hoover FBI Many of these instances were the result of Presidential directives rather than due process Evidence related by Whitfield Diffie, Susan Landau, and Dorothy Denning show that this practice continues to occur in perhaps 50% of the authorized wiretaps granted today

of health data outside the doctor patient relationship of confidentiality Most, however, represent an exchange of information willingly Once one chooses to exit his private world and partake of the greater society, individuals expectations of privacy are forfeit

No Constitutional protections govern the transaction of individuals with independent business Our enumerated protections prevent government intrusions, not commercial ones The popularly accepted notion that we enjoy a "right to privacy" does not apply in our transactions with VISA, MasterCard, L L Bean, Microsoft, Newsweek magazine, or any other business with whom we choose to deal

This is particularly true on the Internet, where electronic commerce has developed the automated data form that will provide services only when mandatory fields of personal data are provided in exchange Willingly entering this transactional world of markets and statistics invites attention How can one claim the benefits of this convenience without recognizing the exchange of privacy privileges inherent in it?

There is a paradox of human nature cited by George Bidzos that we accept risks to our safety in exchange for greater freedom [41] A corollary might be that we accept reductions in our privacy in exchange for convenience In both cases, the choice is still ours to select But privacy arguments weaken when adherents claim an inherent right beyond the enumerated protections embodied in our Constitution and the laws surrounding it

On balance, privacy concerns are valid There is a Constitutional mandate to preserve individuals' rights to be left alone by government agencies The Supreme Court has ruled clearly on this matter But this guarantee is not absolute The courts have provided rulings that promote

[41] George Bidzos, Interview in CNET, January 1998

public safety concerns and balanced these against individual rights Also, there are no clear rights to privacy from business and commercial interests This is particularly true when people remember that an element of choice proceeds any business dealing in which personal information is first exchanged

## Business Interests

Data protection, software application uniformity, and commercial transaction security are the three areas that businesses argue require the unencumbered uses of encryption While businesses have found natural allies among privacy advocates and academics, the nature of these arguments is more purely commercially motivated.

Business data protection is not as threatened as business would have us believe The ability to use a non encrypted yet highly secured file system exists and can be leveraged throughout an enterprise When businesses claim a need for encryption it is to facilitate the transmission of business data across non secure lines of communications rather than to simply protect it in storage

The issue of storage vulnerability does add another layer to the desire for strong encryption products for business uses and would permit concepts like Virtual Public Networks (VPN) to be more viable It would also permit efficient reduction of other more costly and resource consuming security systems such as armed guards, perimeter security electronics and computer firewall systems, each of which has high costs relative to the utility gained by their use

The idea of protecting data and information is not in dispute The FBI does not target legitimate businesses for restrictive measures Strong, domestically available encryption can still be purchased or developed privately for relatively small costs Businesses sacrifice the convenience of ready data access and inter-operability with other businesses, such as suppliers and customers, when the interaction of privately developed encryption schemes with other computer software products becomes cumbersome

The critical problem for U S firms under the current export rules is the inability to deploy a

common business standard across international lines As long as encryption (above 40 bit strengths) is restricted from export, multi-national firms will face the inefficient process of fielding potentially incompatible protection products among their business offices

One possible solution for specific businesses is to obtain export license exceptions that permit the use of 128 bit encryption worldwide subject to restrictions on its deployment, control and disposal and a promise not to sell or transfer the technology to others

Banks currently enjoy this solution offered by the Commerce Department Other companies have applied for and quietly been authorized similar treatment Its only disadvantage is the case by case determination process, which slows the system noticeably at a time when businesses wish to move quickly

This is not a long term solution, however, since neither the Department of Commerce nor businesses wish to prolong a tedious process if a better solution is possible Hence, the push by businesses to lift export restrictions

The second aspect of business objections to encryption controls is argued by those commercial businesses making and selling encryption themselves for mass marketing Product competition among businesses is both keen and, paradoxically, cooperative At any level of encryption the standards across platforms must be fairly uniform to be practical Platform and algorithm transparency is a goal of the Internet community

Consider this in light of the history of electronic word processors Despite differences in speed, efficiency, specific features, and "look and feel," most word processors now inter-operate The software community, after an initial period of stiff competition recognized the utility of inter-operable systems With encryption products, characteristics of speed, disk space requirements,

and throughput times will be the measures of desirability that differentiate products The fundamental algorithms will be similar, nonetheless

So the pressure is high to be the first to field a particular new product line both domestically and worldwide The company that accomplishes this gains the advantage of an installed base from which upgrades and complementary products can be sold This becomes the real issue behind the software companies' desire to lift restrictions

But U S firms already enjoy two of these advantages First market share for U S software products is about 95% worldwide This translates into an installed base of some 80 million or more systems that cannot readily shift away from U S products

Are there real competitors out there? Yes, a few But these are unlikely to steal U S market for encryption in the short term The U S established 56 bit DES is still the worldwide standard even where it is unavailable Even 40 bit systems migrating across foreign markets are generally the U S 's foreign distribution version of a similar domestic product Although Germany, France and the United Kingdom are marketing alternative products, there is a limited demand for non-U S produced solutions And this is usually because of the installed base of application software that only operates well with encryption systems written directly to their software architecture

The remaining concern of commercial businesses is to provide for secure electronic transactions during the buying and selling of services and products Electronic Commerce, where the melding of private and commercial interests occurs, provides the most compelling reason to lift U S export restrictions Safe electronic transactions are a must Uniform, software based encryption is the enabling technology that will permit this to happen Export restrictions slow the growth of electronic commerce and global economic development This is what many businesses

argue Therefore, a promotion of global commerce demands a corresponding support for the mechanisms that enhance such growth

Supporting businesses' needs to secure transactions would be the lever to lift export restrictions and deploy strong encryption worldwide The alternative, to demand key recovery in exchange for export licenses, gives rise to the obvious fear of most businesses Nobody will buy a tainted product Key escrow schemes taint the encryption product to the point that most users will avoid escrowed versions If there is room for a compromise solution, the administration will probably compromise on this aspect of the debate

## Administration Policy Conflicts

The Clinton Administration has published two key policy pieces regarding encryption The Framework for Electronic Commerce and the Administration Statement on Commercial Encryption Yet its actions belie its words According to Brockton Meeks, correspondent for MSNBC (an online outlet of Microsoft in partnership with NBC news), the Clinton record for privacy is dismal

> *One of the most puzzling aspects of the Clinton administration has been its willingness to support the FBI's wholesale demands for the right to strip Americans of their right to privacy in personal communications From telephone calls to electronic mail messages, the FBI, supported by the White House, has sought for and received, to large degree, the ability to snoop on you whenever and where ever they choose It started with the so called digital telephony bill This gave law enforcement officials wide ranging powers to easily tap into telephone conversations. The Clinton administration is in a wiretap frenzy, it has broken all records for allowing taps on the grounds of national security for which no probable cause of a crime is needed. For the first time in history the feds are tapping lines at rate greater than that of cops in all 50 states combined. It's been more important for the president to look tough on crime than as a supporter of civil liberties* [42]

~~Expediency seems to be the watchword for administration guidance on this matter. While the~~ IITF and the EOP both seek to promote electronic commerce and security, the public actions of the President and his policy approaches are at odds Until Congress acts to define the issue, it is unlikely the White House will select an alternative

Two areas where potential policy guidance is more apparent are the use of government buying power to create the de facto standard in software and the publication of the FIPS (see glossary) for key recovery The administration's logic goes something like this if government is the largest

[42] Brockton Meeks, "Good Karma Gone Bad", MSNBC Opinions, February 18,1998

customer and requires key escrow compatible products, then other methods will not successfully gain market shares [43] The FIPS accomplishes the same result for technology developers as the market share argument does for consumers Both approaches have failed, so far, to generate widespread adaptation of the escrowed key approach, yet the administration remains committed to it, apparently

Ira Magaziner represents, for the Clinton Administration, a potential savior He has moved back into the White House after the failed health care initiatives of the first administration to take over policy planning for encryption matters and to articulate a vision for the Internet and electronic commerce

Magaziner views the administration's policy on encryption as a moving target, noting, "On one hand, you need a high level of encryption for electronic commerce On the other, law enforcement thinks crime will flourish We will need to eventually allow some balance between legitimate law enforcement interests and commercial interests We haven't reached the right balance yet in Congress "[44]

Magaziner needs to help the administration build a legal framework that would allow the market to drive the Internet, and ultimately allow the Internet to support a global marketplace He has a deadline of Jan 1, 2000, to have at least a working framework covering the U S position on cryptography, electronic commerce and legal issues, such as intellectual property His goal is to build a consensus among the government agencies working on the issue, in addition

[43] Whitfield Diffie and Susan Landau, op cit p xxx

[44] Ira Magaziner, personal communication, December 1997 (the interview included a hand out of notes from interviews Magaziner gave to various news media at the same time )

to getting local and state governments, the Internet community, and foreign nations to adopt the framework It is unlikely, however, that Congress will provide that much time for his efforts to succeed before acting with legislation

## Minor Interests

The Department of Commerce is not really an advocate for business when it comes to export control of encryption Officials claim to be quietly working to loosen controls Some evidence is clear The exceptions for 128 bit encryption to foreign offices of U S multinational is an example Overall they merely administer the current policy, hiding behind the DoD export veto when necessary

Likewise NIST is weakened in carrying out its duties under the Computer Security Act since it lacks the enforcement authority and the budget to take a lead role No matter what the law says, NIST is unable to counter the NSA's existing advantage in experience, budget or clout when it comes to matters of computers and security

Neither the parent agency nor the subordinate one will determine the outcome of the issues, but both have a stake in the result The Department of Commerce has the goal of promoting the global economy to the advantage of the United States This is enhanced if secure electronic commerce becomes a global activity NIST has suffered from a lack of funds, expertise, and clout when pursuing its mandate to develop and control standards for domestic, non-Defense related computer issues The outcome of the encryption control debate will either leave them a small role, subject to assistance and control from the NSA hierarchy or can permit them to grow into the role envisioned by the Computer Security Act

## National Security Agency Interests

The NSA is of two minds On the public front it maintains that the use of public cryptology is harmful to national security Privately it admits that the nature of NSA's work and the challenge posed by the widespread adoption of commercial encryption does not change the NSA's burden whether the U S policy is restrictive or open

Its stated goals are threefold 1) promote the uses of strong domestic encryption products, 2) assist law enforcement agencies to maintain the status quo of authorized access to communicated information, and 3) preserve export controls [45] This mirrors the administrations stated policies It maintains the argument that foreign access to strong encryption can undermine U S security interests

Reading the contents of an intercepted signal is the most important aspect of cryptology There are, however, other techniques that contribute to the overall effort to analyze intercepted data Rejection of encrypted traffic based on knowledge of the source often obviates the need to decode at all [46]

---

It is also clear, when one can find an NSA official who can discuss the matter frankly, that the decryption challenge can be met, even without the availability of key recovery mechanisms This is time consuming and resource intensive According to one official, "With source codes available,

---

[45] Personal communication with NSA official, April 1998

[46] Among those commenting on this issue, Diffie-Landau, in their recent book argue that traffic analysis provides the most useful indicators of threatening intent They use this argument to undercut the need for decrypted traffic The other side of this argument is that NSA need not obtain evidence admissible in court, thus, the ability to decrypt is not the only useful measure of the value of information Law enforcement proponents point out that admissibility of evidence is crucial

there are many things we can do "[47]

The NSA does, however, have both a Constitutional mandate to provide for the common defense and a strong law, the National Security Act of 1947, to justify its position as arbiter of classified security matters To this end, much of the testimony before Congress during last year's encryption debates was secret When the subcommittee on national security reported out the Goodlatte bill in altered form, it was assumed to be because some classified knowledge was briefed during the closed session

But the classified issues are not germane, according to the NRC panel which studied the issue and included 13 members of the classified information fraternity [48] It is more likely the NSA merely expressed its desire to see commercial encryption emerge more slowly in the marketplace than that it tried to stop it all together

[47] Personal communication with NSA official, November 1997

[48] National Research Council Report, p 13

## Law Enforcement Interests

It is clear to the most casual observer that after spending several years understanding the problem, the FBI wants a very broad law enforcement mandate with regard to encryption technology control It has emerged as the point agency to argue against the private and commercial uses of encryption by both citizens and corporations, both domestically and abroad

But there is no constitutional mandate for a federal law enforcement agency The matter of civil unrest was to be addressed by calling out the militia if necessary[49] There is, of course, a body of legislation defining the role of federal law enforcement and a general societal mandate The basis for federal law enforcement is nonetheless weaker than the Constitutional protections afforded to both individuals and businesses This is what the Framers wanted The notion of the FBI demanding strict federal restrictions against a commercial product is at odds with the concept of both personal liberties and the Commerce clause of the Constitution

There is a common fallacy to deduce that if someone must hide something then one is guilty of something The fact that no one ever needs to justify personal choices doesn't ring true in practice A currently serving U S Attorney stated baldly that when it comes to Department of Justice targets for wiretap or other electronic surveillance means, "There are no innocent victims No one is targeted unless he is guilty of something "[50]

There is a tendency to depict the law enforcement community in a terribly negative light based on the published history of their failures, particularly the harassment of targets who never are charged with a crime While numerous studies and reports, especially the Church Commission in

[49] U S Constitution, Article I, Section 8

[50] Personal communication, unattributable

1976, show a record of law enforcement's abuse of private rights, there are limited defenses of the good record compiled by agencies such as the FBI.

Six studies conducted within the law enforcement community record successful uses of broad law enforcement powers without necessarily abusing such powers Unfortunately, these studies are each commissioned and conducted by the FBI, the Department of Justice, or the Inspector General. There are no independently conducted studies that absolve the law enforcement community of the charges that they abuse their powers

In defense of the FBI, however, it is important to point out that the record of public safety in the United States is tilted toward the agency They have far more successful operations than failed ones They are limited in publishing their successes because this undermines their ability to use powerful law enforcement techniques against future criminal activity Negative stories about FBI abuses of civil liberties gain widespread attention The public wishes the record to be free of any abuses This is not practical Mistakes and overzealous efforts to pursue criminals will occasionally result in abused powers

## History of Federal Law Enforcement

The mandate for strong law enforcement arises only in the 20th century Anti labor, anti communism, anti racketeering, Prohibition, World War II, and the Cold War all provided a basis for extending the power of a domestic crime prevention and investigatory body Both Diffie-Landau and Dorothy Denning review the history of local and federal law enforcement during the late-19th century and early 20th century Their most telling points relate to the rise in federally defined crimes that occurred after the 18th Amendment (Prohibition) and continued to rise as more and more items were added to the list of federal crimes As with any burgeoning bureaucracy,

however, abuses were inevitable, whether these were inadvertent or malicious

The Congress and the Courts have responded to past abuses with restrictive rulings and laws designed to curb excesses while continuing to promote strong federal law enforcement The riots and anti war protests of the 60's provided the modern leaning of government toward permitting more encroachment by law enforcement into personal liberties Finally, the war on drugs and the "tough on crime" attitudes of the 80's provided a solid basis for today's climate that the federal law enforcement community has a strong anti-crime mandate

What role should law enforcement play in the encryption debate? Advocates for a strong role argue that crime prevention is a primary function of the federal law enforcement community To accomplish this it requires broad powers to interdict potential crimes before they are committed Encryption of conversations and documents hinders this

Regardless of the obstacle encryption might pose, long before the FBI obtains a legal wiretap or electronic surveillance it must have some compelling evidence that a crime is imminent It must apply for a warrant through a supervisor, a Deputy Assistant Attorney General, and a federal judge Surely, if the FBI can convince these persons that a crime is imminent, its encounter with encrypted communications does not destroy the case It might make investigative timing and arrest problematic, but that is another matter Simply put, evidence of a conspiracy to commit a crime seldom originates as a result of electronic surveillance [51] The surveillance cannot in fact exist until evidence of a crime precedes it So the crime prevention portion of the FBI's argument is weakened

[51] Best argued by Dorothy Denning in her 1997 article in Educom Review, but also contained in the Omnibus Crime Control and Safe Streets Act record of debate and in the Church Commission report

A stronger argument can be made for the case of crime investigation In these cases some criminal act has occurred and the FBI is obtaining evidence from a variety of sources Physical and the forensic evidence derived from it is the most compelling information law enforcement can provide to prosecutors Next are confessions, accomplice statements, and witness statements Phone records, computer files and electronic data are a third, but less compelling form of evidence If these latter are encrypted it does indeed hurt the mission of the FBI in solving a crime But this has not been a fatal flaw of prosecuting crime, yet

What is likely, however, is that in gathering the evidence, law enforcement officials ultimately obtain the key to encrypted data during the same searches that develop other forms of evidence Even was the key hidden elsewhere, cracking a computer file is not an impossible job (see NSA analysis), albeit a time consuming and expensive undertaking Finally, if the encrypted files remain unopened, it is unlikely (and never true yet) that the FBI lacks enough evidence to prosecute the case any way [52]

An analysis of the cases involving computer files and private communications since 1986 shows two things First, no crime has gone unprosecuted because of encrypted files or communications, despite FBI Director Freeh's claims to the contrary Second, wiretaps and other surveillance that may be affected by encryption are the least important evidence at trial Physical and other forms of evidence tend to be overwhelmingly conclusive Additionally, analysis has indicated that electronic surveillance is the least cost effective means of evidence gathering [53]

The FBI argues another line as well It states that restricting encryption merely maintains the

[52] Dorothy Denning, The Future of Cryptography, January 1996

[53] Dorothy Denning, Cases Involving Encryption in Crime and Terrorism, October 1997

status quo of powers already granted This fails to stand up to examination Encryption involving key recovery goes beyond the wiretap example since it demands a prior and unrevocable deposit of crypto keys and a built-in capability to eavesdrop on communications Wiretap authority specifically limits the time, place, and content of what is being obtained to the specifics of the warrant application

Additionally, wiretap authority permits the police to listen but does not guarantee they will obtain any useful information, nor does it permit an unlimited wiretap until useful information is gained The courts have been very specific in controlling just how the police can obtain and use wiretap data, particularly preventing them from engaging in "fishing trips" [54] Key recovery permits both the unlimited gathering[55] and a guarantee of deciphering the content This is well beyond the status quo which the FBI argues it wishes to maintain

Finally, the cost of law enforcement has only been indirectly passed to the people since it is taxpayer funded Digital telephony and key recovery schemes require the users of encryption and the infrastructure required to maintain the recovery mechanism be paid for by the target themselves This is arguably a new violation of the 5th and 6th Amendments according to Froomkin, although no cases have yet reached the courts

The Courts are unlikely to find the funding of new law enforcement mechanisms to be a matter of great concern The Congress, however, may well reconsider this aspect of the emerging policy

[54] Froomkin, op cit p 792

[55] Key recovery permits the surveillant to decrypt all traffic obtained within the time limit of the court order The key provides this level of access In the case of wiretap, the court orders require the tapes to be turned off when non-relevant conversations or those involving non-targets occur Such protection does not happen with decryption Arguably, innocent persons are now subject to unintended surveillance

as it did when Digital Telephony was first defeated in 1993 The resulting act in 1994 provided government funds to cover the expense of converting telephonic switches to the government mandated configuration

Generally, there is a large body of solid law that permits a broad law enforcement involvement in areas that infringe civil liberties Since the 1980's the balance has shifted from a protection of individual rights to a "war on crime" Both the courts and the Congress have contributed to this shift There is also a large body of law and court rulings that favor free business activities Along the line of intersection, the current key recovery, encryption control debate appears to be carving new concepts between law enforcement needs and business freedoms Individual rights are recognized but subordinate to these other interests

## Conclusions

The interests examined in the preceding pages represent the main parties involved in the current encryption technology control debate There are fundamental differences in opinions about civil liberties, law enforcement, national security, and business markets

Privately developed encryption is available Individuals and businesses have the wherewithal to obtain or to write for themselves effective encryption schemes rather than to buy them commercially This is not convenient, of course It prevents widespread uses such as providing Internet security or e-mail protection unless the owner delivers a copy of the scheme to the recipient(s) prior to the encrypted communication It is, however, a possibility that many individuals and companies can choose if they wish to avoid the key recovery schemes that may be required of commercial products It is also the alternative businesses fear will be employed by foreign competitors Finally, it is the probable alternative criminals will choose if key recovery is required for commercial systems

Business interests in free market deployment and use of commercial products to support secure electronic commerce might tip the scale against the successful implementation of key recovery schemes There is a strong pro-business element of both the administration and the Congress toward promoting economic activity

The NSA has maintained its interest in the debate, but has let the Department of Justice lead the fight for tougher controls This is probably because many within NSA see the inevitability of encryption migrating worldwide, with or without U S controls Since NSA must perform its mission regardless of the challenges, it appears to be quietly preparing to tackle the encryption that will appear, rather than expend energy in the Congressional debates

Law enforcement will continue to receive wiretap and electronic surveillance approvals under the current law without regard to the encryption issue It remains to be seen if the pro-law enforcement members of the Congress defeat the pro-civil liberties forces sponsoring such bills as SAFE If the FBI succeeds in obtaining key recovery provisions, business and individual freedoms are at further risk, but actual losses are likely to be no different from what is now the case

If the policy or law enacted requires key recovery for encryption controls, judges are likely to support the constitutionality of such measures Froomkin's analysis indicates that such measures are not intrusive enough to merit judicial protection of individual freedoms Protection of the public safety from crime tends to over ride personal freedoms

The Congress is difficult to predict There are strong civil liberties advocates as well as pro-law enforcement and pro-business elements A renewed version of SAFE will probably be the model of legislative measures in 1998

Compromise is difficult to find when the positions involved are so opposed What law enforcement claims is directly opposite from what privacy advocates demand Key recovery works directly against free market determination of encryption sales shares One alternative, the key recovery approach, threatens to limit the deployment of uniform Internet security standards in support of electronic commerce as well as to threaten privacy The opposite approach, to promote free encryption deployment worldwide lessens the ability of law enforcement to determine the nature and timing of a potential crime If such a crime is a terrorist threat or attack, failure to prevent it because of strong encryption would likely lead to a public backlash against the technology

Individuals concerned with personal privacy will probably have to live with whatever business

interests and government leaders eventually agree to do A compromise is most likely between business and government since economic impacts are readily calculated and directly felt by politicians This can favor individual rights, however, since many of the aims of business coincide with individual concerns

## Chapter 3.

## A National Encryption Strategy

### Elements of a National Strategy

If we take the administration at face value, based on the Framework for Electronic Commerce and the statements of both Al Gore and Ira Magaziner, we can envision a future time when unencumbered encryption exists, freely distributed worldwide It enables secure transactions across the Internet, it protects personal and business communications and records Yet it poses no threat to the status quo of law enforcement methods for crime prevention and investigation nor threats to national security

If this is indeed what the administration wishes to achieve, then one approach is to ignore for the moment the barriers now apparent and formulate a strategic model that achieves this goal If we develop such a strategy successfully, then a series of policies should follow that protect individual rights, enhance commerce, and foster public safety domestically and internationally without conflict

The framework for this approach requires us to first ignore the existing barriers First visualize the perfect future state Widespread encryption, free of escrowed key recovery (because this is not acceptable to the primary users), yet providing a means for law enforcement and national security elements to continue successfully at their public safety mission How do we reach this goal?

The second step is to identify both the opportunities to achieve this vision and [now] the barriers to its successful implementation Finally, examining the risks and costs associated with the approach permits us to realistically evaluate the vision

There is no doubt that national security threats still exist But are they insurmountable? This is no longer the Cold War era when instantaneous decision making is necessary to control events or avert disaster Threats now tend to involve either long term economic goals or short duration terrorist and thug actions, especially those involving weapons of mass destruction The question then is how do we mitigate the need to obtain knowledge of potential threats if encryption is prevalent?

If mandatory key recovery is untenable as a means to achieve the vision, the remaining approach is to devote more resources to source code analysis and increase the chances for decoding successes Intercepting, analyzing source data, signal data, traffic patterns and message sizes all contribute to the business of understanding encrypted information, yet none of these methods require a plaintext solution Even without the powerful value of plain text decrypted messages, much knowledge can be gained about intercepted signals As the NSA official pointed out, " there are things we can do " with source codes

Ultimately, NSA might require a plaintext decryption of a few potentially threatening messages To provide for this, the tools of code breaking need enhancement Brute force methods are deemed impossible once key lengths reach 64 bits But other techniques still remain viable Obtaining the keys, obviously provides a solution Deciphering through direct (brute force) analysis can succeed Access to the software source code of the program used to encrypt a

communication provides additional assistance [56] Our model of unencumbered encryption usage requires a resource shift from maintaining a key recovery based, trusted network to providing more tools and support to existing agencies responsible for decoding encrypted data True, real time decoding is not enhanced by this approach But this does not differ from the current case when NSA encounters foreign codes for which it has no keys This solution still maintains the status quo

The situation is analogous for law enforcement needs First, is an increase in crime likely when encrypted communication deploys widely? This is a debatable point Crime rates will probably follow their historic trends without regard to the uses of encryption Encryption does not enhance committing crime, it only helps to hide crime or to hinder evidence gathering Indeed, the widespread use of encryption can potentially reduce the number of data targets available to the criminal Since encryption that poses such a problem to law enforcement undoubtedly poses a greater problem for criminal elements there is a balance between supporting encryption for data protection against restricting it to enhance crime solving

A solution for law enforcement, then, is to continue with existing wiretap and surveillance practices Analyze traffic sources, signal data, and other "tell tales" for appropriate clues, then focus resources on decoding only potentially high value messages (based on the value assessed to the circumstances surrounding the interception) Again obtaining the key via court ordered search or subpoena is a first step, particularly since most keys are found on the same media as the

[56] The availability of source code to an encryption algorithm speeds the process of decryption somewhat Regardless, according to a variety of experts, the absence of the session key requires strong computing power and time in order to decrypt information Key length remains the fundamental determinant of successful decryption

encrypted data Next decoding or code analysis is appropriate Again, real time decoding is not enhanced, but is less fatal to law enforcement than is believed (or than the record indicates) Finally, of course, developing other related but unencrypted evidence is always appropriate The essence of this approach is to attack crime with a better use of existing tools and when warranted, to crack codes with additional effort

Resources must be devoted to this approach. The National Computer Crime Lab, in cooperation with the National Security Agency and military expertise provide a basis for such an improved capability The PCCIP hinted that such an agency was potentially important (see Article PCCIP and the NIAA) The FBI recently obtained purview to run the National Infrastructure Protection Center, a focal point for protecting U S domestic interests These resources permit the application of greater effort to efficiently investigate and attack the encryption challenge

Absent key recovery schemes, both individuals and businesses are no longer adversaries to administration policy toward encryption technology Essentially, these interest groups receive what they demand Taxpayers, however, have to foot the bill for new resources devoted to encryption issues This is where a potentially new compromise comes into play

**A Proposal for Encryption Strategy**

If software developers agreed to escrow not the keys, but the source codes of their products and in return received unrestricted freedom to export strong encryption worldwide while pursuing free market strategies for their products, a smaller trusted agency would be capable of maintaining the proprietary interests of businesses(similar to patent and copyright protections) while acting as the gatekeepers for national security or law enforcement access to these source codes Source codes themselves do not guarantee successful decryption, but according to NSA spokespersons,

contribute toward reducing the burden of decryption efforts

Separation of interests between law enforcement and trusted agents would be inherent But armed with judicial approval, law enforcement could access the source code from the escrow location and use it to assist in the code breaking , if this became necessary during the pursuit of a potential criminal enterprise While not providing instant decoding capability, NSA experts agree that access to the source code provides, "things we can work with "[57] If NSA were provided enabling legislation to expand their assistance to law enforcement even, a potential to protect privacy while assisting law enforcement interests exists

Additionally, to fund this approach, a software sales surcharge can be imposed on buyers of encryption products Set at an amount fair to the buyer and capable of funding the trusted system, it might amount to $1 to $5 per sale This could generate up substantial sums over time to provide law enforcement with enhanced tools to collect and analyze legitimately suspect communications

This approach preserves the freedom of individuals while permitting choice, but with the voluntary recognition that this freedom indeed has a cost It promotes world markets for business It addresses law enforcement concerns, albeit to a lesser degree than they demand But approaching the degree to which the documented problem actually exists

Combining competing interests in this way mitigates the arguments while maintaining a reasonable means to prevent catastrophic crime or the erosion of freedoms Policies which result from this over arching strategy achieve the goals identified in the Introduction to this report

**Policy Models**

[57] Personal communication with NSA personnel

First, policy for cryptology as part of private communications is supported Individual freedoms from unlimited intrusion by government are protected A reasonable expectation of privacy is maintained Choice of the methods, products, and implementation of encryption schemes are entirely open to the individual Costs are reasonably covered by a surcharge on each purchase of encryption capable software or hardware Frequency and degree of use remain matters of individual choice

Second, policy for cryptology as part of business use and electronic commerce will follow an open market model Domestic sales of encryption capable hardware and software are unrestricted A surcharge on each sale can be absorbed by either the manufacturer, the distributor or the purchasers as market forces determine Voluntary disclosure and escrow storage of source code for domestic uses is encouraged but not required Export licenses will be granted for unrestricted worldwide distribution of encryption products subject to the mandatory escrow of the source code Absent an escrow agreement, restricted licenses will be granted for products with capabilities not to exceed 56 bit key lengths Surcharges are payable following the final sale, not at the time of export

Third, policy for cryptology as part of national security will continue as it has for many years The Central Intelligence Agency, the Department of Defense, and the Department of State will maintain their capabilities to protect national interests Improvements to infrastructure and intelligence activities in the face of increasingly worldwide deployment of encryption technologies will be a matter of budgetary and planning interest The existing capabilities to intercept, analyze, decode and exploit encrypted traffic will be enhanced

Fourth, policies for cryptology as part of law enforcement will enhance the ability of domestic

law enforcement to collect information, investigate, and prosecute criminal activities which might use encryption technology or electronic media The Joint National Electronic Crime Lab (JNECL)[58] under the auspices of the Department of Justice and the Department of Defense will exploit domestic intelligence, promote infrastructure protection, and develop crime information The FBI will be the executive agent of the JNECL and will budget and plan for its activities NSA will provide expertise and facilities to complement the needs of the law enforcement community Such efforts will be funded by the software surcharge and permitted by enabling legislation to loosen restrictions on NSA to law enforcement cooperation

Fifth, policy for access to source codes, maintained by a trusted agency on behalf of the business community will mirror the policies for wiretap and electronic surveillance embodied in the Omnibus Crime Control and Safe Streets Act of 1968, as amended

[58] At this time the National Infrastructure Protection Center provides a model for this future agency

## Conclusion

Such a plan can achieve the vision of unencumbered encryption product availability It requires a compromise by businesses, in providing their source codes outside of proprietary business channels, as well as a compromise from law enforcement, to reduce its desire to have unencumbered access to personal communications It preserves civil liberties and protects citizens from potential abuses

It requires leadership and courage to advocate a position that necessarily avoids giving any group everything it wishes to achieve It moves the debate away from the potentially paralyzing impasse in which it now is mired It recognizes the potential ubiquity of new technology to permeate our lives whether we are prepared to adjust to it or not

# Appendix A A Cryptology Tutorial

Appendix A. A Cryptology Tutorial

Before the invention of public-key cryptography in 1976, a sender and receiver who wanted to use a cipher had to agree on a key in order to communicate securely But first, sender and receiver needed a secure means to transmit the key itself! Second, even if the key was transmitted securely, the security of a single-key cipher evaporated as soon as the key was compromised Third, the ever-present danger of key compromise cast a doubt over the authenticity of every message

Public-key cryptography solves all of these problems In a public-key system, each user creates a public key, which is published, and a private key, which is absolutely secret Messages encrypted with one key can be decrypted only with the other key, and vice-versa

Thus, if Alice wants to send a secure e-mail message to Bob (by some strange convention Alice and Bob are the industries' fall guys for all sample exchanges), and they both use compatible public-key cryptographic software, Alice and Bob can exchange public keys on an insecure line It is easy to establish a secure line of communication with anyone who is capable of implementing the algorithm

One drawback, however, is that public-key encryption and decryption is much slower than commonly used single-key systems such as DES The speed problem can be overcome, however, by using a hybrid system Public-key cryptography allows Alice and Bob to achieve this feat in either of two ways Using the first method, Alice generates a session key, encrypts it with Bob's public key, and sends it to him Bob decrypts the message with his private key, inputs the session key to his single-key software or telephone, and then the data exchange or conversation begins Alternatively, the parties can use Diffie-Hellman Key Exchange (see following text)

As a result, all that Bob needs in order to send Alice a secure e-mail is a reliable way of getting Alice's public key Key servers provide a simple way of making public keys generally available Essentially, a key server is a computer with a white pages approach to public key management Bob enters Alice's name and the key server replies with Alice's public key-- if she has registered it Key servers generally work on one of two principles the certification authority or the web of trust. Under the certification authority paradigm, some central body authenticates the identity of the registrant when the key is first deposited By contrast, there is no central authority for web-of-trust The web-of- trust approach is, however, the foundation of the PGP encryption system which is also now the most ubiquitous

# DIFFIE-HELLMAN

Diffie-Hellman key exchange is a public-key technique that takes advantage of the fact that it is easy to compute powers in modular arithmetic, but very difficult to extract logarithms If $y$ is the $x$th power of $b$, modulo $p$

$$y = b^x \pmod p$$

where b is a suitable base number, then, as in ordinary arithmetic, $x$ is the logarithm of $y$ to the base $b$, modulo $p$

$$x = \log_b y \pmod p$$

Calculation of $y$ from $x$ is easy, but computing $x$ from $y$ is difficult In the following illustration using exponential key exchange to establish session keys, the equipment being used to carry out the key distribution is personified as Alice and Bob, just as if the users were doing the computing in their heads

The base $b$ is known to both users To initiate communication, Alice chooses a random number $A$ She keeps $A$ secret, but sends

$$b^A \pmod p$$

to Bob Bob in turn chooses a random number, $B$, and sends the corresponding $b^B$ to Alice Both Alice and Bob can now compute

$$b^{AB} \pmod p$$

~~and use this as their key Bob computes $b^{AB}$ by raising the $b^A$ he obtained from Alice to his secret~~ power $B$

$$(b^A)^B \pmod p = b^{AB} \pmod p$$

Similarly, Alice obtains $(b^B)^A = b^{AB}$ Only Alice and Bob know the secret value $b^{AB}$ There is no known way for anyone who does not know either $A$ or $B$ to compute $b^{AB}$ without first attacking the difficult problem of taking the logarithm of $b^A$ or $b^B$

If $p$ is a prime about 1,000 bits in length, only about 2,000 multiplications of 1000-bit numbers are required to compute the exponentiation By contrast, the fastest techniques for taking logarithms in arithmetic modulo $p$ currently demand more than $2^{100}$ (or approximately $10^{30}$) operations Even with today's supercomputers, it would take a billion billion years to perform this many operations

# Appendix B A Chronology of the Cryptology Issues

## Appendix B A Chronology of the Cryptology Issues

1940-1945 -Enigma, Ultra, and Magic systems used by US/UK

1940 to1970s -U S government maintains a practical monopoly on cryptology technologies

1973 -National Institute of Standards and Technology (NIST) issues request for proposals for Digital Encryption Standard (DES)
1974 -NIST issues new RFP for DES following non-response from industry
1976 -Public Key cryptography goes public RSA standard proposed
1977 -DES published as standard
1978 -Government Accounting Office reviews complaints about DES process States the process was conducted properly

1982 -NIST solicits public key algorithms for use in a new standard
1983 -DES reaffirmed
1984 -National Security Decision Directive (NSDD) 145/14, by DoD, requires that all electronic security systems be reviewed by the National Security Agency (NSA)
1985 - NSA announces DES expiration in 1987
-GAO reports a conflict within NSDD 145/14 between domestic government agency needs, defense and security needs, and commercial financial security issues
1986 -Federal Bureau of Investigation reviews wiretap capability versus emerging encryption technologies
1987 -DES recommended for banking uses only
-NSA requests end to public key project at NIST
-Computer Security Act moves authority to regulate electronic technologies to Department of Commerce (NIST)
1989 -Commerce and NSA sign Memorandum Of Understanding (MOU) giving NSA final approval of electronic technology issues and solutions
-NIST and NSA develop Federal Information Processing Standard 185 for public key systems development

1990
May -FBI begins wiretap capability improvement study
Nov -President issues executive order moving dual use technologies from State Department export control to Commerce export control

1991
Jan -Senator Biden Introduces S 266, The Comprehensive Counter Terrorism Act of 1991 which addressed encryption issues
Apr - after much debate among State, Defense, and Commerce, encryption remains on State Department export control list
June -S 266 withdrawn

Aug - NIST introduces Digital Signature Standard (DSS)
Oct - Rep Levine introduces amendment to limit export controls for dual use items

1992
Jan -NIST reviews DES
Jan -Encryption export control again moved to Commerce, again rescinded by DoD
Jul - Digital telephony proposals by FBI to Senate, no bill introduced
Jul -Commerce/State Department approve 40 bit key exports

1993
Apr -White House announces Clipper Chip, a hardware based, proprietary encryption device
Jul -NIST proposes FIP185 for key escrow systems
Oct -SKIPJACK proposal for key escrow systems It is proprietary hardware
Nov -GAO report released reviewing government actions regarding encryption since 1973
Nov -Rep Cantwell introduces bill to relax export controls of cryptography
Dec -DES recertified by NIST

1994
Feb -White House announces official adoption of Clipper Chip
Apr -Cantwell bill voted down by House Intelligence Committee
Apr -Vice President Gore suggests development of software key escrow systems
Jun -Association of Computing Machinery (ACM) report released, reviews issues but offers no recommendations
Sep -Office of Technology Assessment (OTA) report released, reviews issues but offers no recommendations
Oct -FBI Digital Telephony bill signed into law Requires telecommunications industry to build wiretap access into networks

---

1995
Nov -Proposed NIST software Key Escrow Encryption Standard, November 1995

1996
Jan -Department of Justice drops investigation of Phil Zimmermann for lack of evidence
Mar -Senator Burns introduces S 1726 to relax export controls
-Senator Leahy introduces the Encrypted Communications Privacy Act, S 1587
-Rep Goodlatte introduces the Security and Freedom through Encryption Act, H R. 3011
May -National Research Council (NRC) report released Recommends staged relaxation of export control No key escrow endorsements Let public set limits
Oct -104th Congress Ends without passage of bills
Nov -Executive Order directs export control of encryption under Commerce

1997
Feb -Congressman Bob Goodlatte introduced H R 695, Security and Freedom Through

Encryption (SAFE) Act

Feb -Senator Patrick Leahy Introduced S 376 (later S 909), Encrypted Communications Privacy Act

-Senator Conrad Burns introduced S 377, The Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act

Aug -Encryption bill proponents and opponents draw battle lines, staged press coverage daily

-Federal District Court, San Francisco rules against government in Bernstein v State

Sep -FBI proposes domestic encryption controls

-Administration denies domestic controls are official position

-OECD issues anti-encryption controls report

Oct -EC repudiates encryption controls

-France validates strict encryption controls.

-HR.695 to House Rules Committee for review and reconciliation of five versions

-S 909 seems dead in committee

-S 377 still active

-no bills likely to pass this session

-Administration spokesmen admit there is no clear policy yet

Dec -US 9th Circuit hears encryption control appeals

Appendix C Sources Consulted

Appendix C Sources Consulted

Note Sources sub-divided by category Within categories sources are listed chronologically to facilitate an understanding of the evolution of the debate Turabian 7 6 is followed

**Books:**

Thomas Jefferson and George Washington, et al, The Declaration of Independence and the Constitution of the United States of America, Institute for National Strategic Studies reprint, with commentary by Richard D Stevens, U S Government Printing Office, Washington, DC, 1994 edition

Alexander Hamilton, James Madison, and John Jay, The Federalist, Encyclopedia Britannica, Inc reprint, University of Chicago, 1952

Christopher Collier and James Lincoln Collier, Decision in Philadelphia, The Constitutional Convention of 1787, Ballantine Books, Inc , New York, 1986

Alvin and Heidi Toffler, War and Anti-War, Warner Books Inc , New York, 1993

Stuart J D Schwartzstein, ed , The Information Revolution and National Security, The Center for Strategic and International Studies, Washington, DC, 1996

Alan D Campen, Douglas H Dearth, and R Thomas Gooden, eds , CyberWar Security, Strategy, and Conflict in the Information Age, AFCEA International Press, Fairfax, Virginia, May 1996

Frank Fukuyama, Trust The Social Virtues and The Creation of Prosperity, Free Press, New York, 1996

Whitfield Diffie and Susan Landau, Privacy on the Line, The Politics of Wiretapping and Encryption, MIT Press, Boston, MA, January 1998

**Reports and Studies:**

General Accounting Office, Communications Privacy Federal Policy and Actions, November 1993

Lance Hoffman et al , Cryptography, Policy and Technology Trends, DE-AC05-840R21400, January 1994

James Bidzos, Some Thoughts on Clipper, March 1994

Association for Computing Machinery, Codes, Keys and Conflicts, June 1994

Office of Technology Assessment, Information Security and Privacy in Network Environments September 1994

Lynn McNulty, secretary, Minutes of the Computer System Security and Privacy Advisory Board, NIST, January 1995

CommerceNet Consortium, Toward Enabling Secure Electronic Commerce The Need for a Revised U.S. Cryptographic Policy , June 1995

A. Michael Froomkin, The Metaphor is the Key. Cryptography, the Clipper Chip and the Constitution, The University of Pennsylvania Law Review, January 1995

A Michael Froomkin, It Came From Planet Clipper, The University of Chicago Legal Forum, Chicago, 1996, (1996 U Chi L Forum 15)

Matt Blaze, et al, Ad Hoc Report, Minimal Key Length for Symmetric Ciphers, January 1996

Dorothy Denning, The Future of Cryptography, January 1996

National Research Council, Cryptography's Role in Securing the Information Society , U S GPO, May 1996

National Research Council, U.S. Policy Should Foster Broad Use of Encryption, U S GPO, May 1996

G A Keyworth and David E Colton, The Computer Revolution, Encryption and True Threats to National Security, Progress and Freedom Foundation, June 1996

William J Clinton and Al Gore, Administration Statement on Commercial Encryption Policy, U S GPO, July 1996

William J Clinton and Al Gore, National Security Strategy Planning Document, U S GPO, March 1997

William J Clinton and Al Gore, A Framework for Global Electronic Commerce, U S GPO, July 1, 1997

Lynn McNulty, secretary, Key Escrow Issues Meeting, Discussion Paper #4, NIST, September 1997

Louis Freeh, The Impact of Encryption on Public Safety, FBI Report, September 1997

The Computer Systems Policy Project, Perspectives On Security In The Information Age , undated reprint found September 1997

Committee on Information and Communications, America in the Age of Information, NSTC, undated reprint found September 1997

Dorothy Denning, Cases Involving Encryption in Crime and Terrorism, October 1997

Shari Steele, Decoding the Encryption Debate, unpublished, undated, received October 1997

Marsh, et al, Presidential Commission for Critical Infrastructure Protection Report, November 1997

Wayne Madsen, Cryptology and Liberty, An International Survey of Encryption Policy, Global Internet Liberty Campaign, http //www gilc org, February 1998

**Articles:**

(Note where source document was on-line no page numbers are available )

Mike Godwin, A Chip Over My Shoulder The Problems with Clipper, Internet World, July 1994

unknown author, Administration Moves Toward Encryption Plan, The Wall Street Journal, July 15, 1996

Bill Gates, Microsoft Policy on Export Controls on Encryption, Microsoft Network, November 1996

Phyllis Schlafly, Encryption is Important to Freedom, Eagle Forum, April 2, 1997

Steven Levy, Bill and Al Get It Right, Newsweek, July 7, 1997, p 80

Tiare Roth, Report Refutes Crypto Rules, C-Net, July 31, 1997

John Ashcroft, Welcoming Big Brother, The Washington Times, August 12, 1997, p A15

Becky Beaupre, Lack of Laws on Net Raises Questions About Privacy, Potomac News, August 19, 1997, p A5

Joshua Quittner, Invasion of Privacy, TIME, August 25, 1997, pp 27-35

Maria Seminerio, Crypto Ruling Impact Debatable, Ziff-Davis Net, August 26, 1997

David Braun, Congress returns to Pressing Tech Issues, TechWire, CMPNet, August 29, 1997

Kate Gerwig, Industry News. Policy Issues, CMPNet, September 1997

Rajiv Chandrasekaran, Freeh Seeks Encryption Decoding Key, The Washington Post, September 4, 1997, p E1

Dan Goodin, White House Shuns FBI Crypto Plan, C-Net, September 5, 1997

author unknown, FBI Crypto Bill Forces Key Recovery, Center for Democracy and Technology, press release, Volume 3, Number 13, September 8, 1997

author unknown, A Step Backwards, Information Technology Association of America, press release, September 9, 1997

Jim Kerstetter, Gore Defends Encryption, PC Week, September 9, 1997

Tim Clark, Gore Calls for Piracy Crackdown, C-Net, September 9, 1997

Rebecca Vesely, Crypto Liberalization Bill Crippled, Wired News, September 9, 1997

Hiawatha Brady, Tales from Encryption, Boston Globe, September 11, 1997

Jim Kerstetter, Looming Encryption Battle Raises Stakes for IT, PC Week, September 12, 1997

Rebecca Vesely, White House Wrangling Over Crypto News, Wired News, September 12, 1997

Dan Goodin, U S Violates Global Crypto Policy, C-Net, September 15, 1997

Jonathon Weber, Encryption Bill, Ignorance Rears Its Head Again, Los Angeles Times, September 15, 1997

author unknown, Magaziner Stumps for Open Internet Marketplace, Media Daily, September 17, 1997

Douglas Hayward, U S Laws Cripple Euros, TechWire, CMPNet, September 17, 1997

John Carey, The FBI Versus Silicon Valley, Business Week, September 18, 1997

author unknown, Crypto Bill Talks Deadlocked, Reuters, September 19, 1997

Rebecca Vesely, Fight Continues for Crypto Bill, Wired News, September 19, 1997

Adam Smith, Encryption Laws Stymie U S Competitiveness, Puget Sound Business Journal, September 22, 1997

John Rendleman, E Commerce Vendors, Users Have an Encryption Conruption, Internet Week, CMPNet, September 22, 1997

author unknown, Bells Oppose Encryption Controls, Reuters, September 23, 1997

author unknown, Privacy Still Valid in Today's Computer Age, Houston Chronicle, September 23, 1997

Eric Wilson, Government Sales Tax Impossible to Administer, Financial Review, Australia, September 23, 1997

author unknown, Scientists Warn Against Encryption Controls, Excite Daily News, September 24, 1997

C Morris, High Speed Data Encryptor, C4I Digest, September 30, 1997

David Winer, Ideas for Privacy, DaveNet News, September 30, 1997

Dorothy Denning, Encryption Technology and Crime, Searching for a Neutral Zone, Educomm Review, September/October 1997, p 39

author unknown, Security Features in Microsoft Mail, MSN, October 1, 1997

Ashley Dunn, Of Keys, Codes, and Personal Privacy, CyberTimes, October 1, 1997

Peter Wayner, Police Versus Us The Encryption Challenge, CyberTimes, October 1, 1997

Courtney Maraunita, High Tech Told to Play Politics, C-Net, October 2, 1997

Dan Goodin, EC Report Counterpoint to Clinton Crypto, C-Net, October 8, 1997

Ashley Dunn, Government and Encryption. Locking You Out, Letting Them In, CyberTimes, October 8, 1997

Ashley Dunn, Secrecy, Privacy, and The State, CyberTimes, October 9, 1997

Jeri Clausing, Market Driven Encryption Policy, CyberTimes, October 9, 1997

David Braun, Encryption Stalemate Threatens E Commerce, National Security, TechWire, CMPNet, October 9, 1997

Margie Semilof, Sun Crypto Chief Speaks Out, TechWire, CMPNet, October 10, 1997

Russ Mitchell, FBI Reading E-Mail, US News and World Report, October 13, 1997

Duncan Campbell, Europe Spikes Spooks E-Mail Eavesdrop Bid, The Guardian, October 15, 1997

Eric Wilson, Impossible to Administer in Borderless Commerce, Australian Financial Times, January 22, 1998

Sara Miles, On Tech Policy, Time to Walk the Walk, Wired News, January 30, 1998

Juliana Gruenwald, Congress Finds No Easy Answers to Internet Controversy, Congressional Quarterly, February 1998

Paul Davidson, Congress Wrestles with Net Restrictions, USA Today, February 9, 1998

Dave Gussow, Taking a Gigabyte Out of Crime, St Petersburg Times, St Petersburg, FL, February 9, 1998

Alex Lash, US One of Few Restricting Crypto, CNET, February 9, 1998

US Crypto Rules Among Most Restrictive, Wired News, February 9, 1998

**Interviews and Personal Communications:**

The Honorable William Reinsch, Deputy Under Secretary of Commerce

Doctor Clinton Brooks, Deputy Director, National Security Agency

Mr John Marvita, Senior Staff Member, U S House of Representatives, Committee on Commerce

Ms Shari Steele, The Electronic Frontier Foundation

Captain Ken Verbruegge (Class of 97), Deputy Director, Information Operations Technology Center, Department of Defense

**Home Pages:**

The Internet Privacy Coalition Information Page, http //www privacy org/ipc

The Electronic Policy Information Center Resource Page, http //www crypto com

The Electronic Frontier Foundation Home Page, http //www eff org

The Electronic Freedom Foundation Home Page, http //www xxx org

Global Internet Liberty Campaign http //www gilc org/

The Office of the President Home Page, http //www eop gov

The Information Infrastructure Task Force Home Page, http //www iitf doc gov

The Cryptology Project, http //www cosc georgetown edu/~denning/crypto

Note Dr Dorothy Denning at Georgetown has an extensive library of articles, reports and studies on-line that deal with this topic in a level of detail much greater than this report can address At the risk of superceding my work, I have summarized the contributions and sources I have obtained from that site under the simple, home page entry above Be assured, it consists of much scholarly work by both Dr Denning and her contemporaries in this area

**NATIONAL DEFENSE UNIVERSITY**

NATIONAL WAR COLLEGE

# CLIPPER CHIP
A Policy Challenge of the Information Age

---

DECEMBER 4, 1997

MICHAEL H CAMILLETTI/CLASS OF 1998

The National Security Policy Process
Course 5603
SEMINAR H

FACULTY SEMINAR LEADER
Dr R McDonald
Dr C Watson
FACULTY ADVISOR
Mr J Stefan

## CLIPPER CHIP

A Policy Challenge of the Information Age

### Introduction

As policies go, there was little wrong with the announcement that the Clipper Chip, a silicon processor capable of encrypting data transmissions, for use in computers, fax machines, and telephones would be made available to the public If anything, government officials were expecting a certain amount of gratitude as they provided a solution to a growing demand for secure information exchange After all, the government had experimented and developed this approach without forcing individual companies to spend their own capital It was a gift from government to those who needed such a product

---

**Brief History of U.S. Cryptology Policy**

*1930-1975 Government monopoly exists Expense and scarcity of computing power make the issue unimportant*

*1976-1990 Public key cryptography arises Costs go down as processing speed goes up 40 bit export limit arises*

*1991-1994 Hardware solutions exist but government controls processes Some exceptional 56 bit exports granted*

***1993 Clipper Chip announced; policy attacked. Debate goes mainstream***

---

So why was there suddenly such an outcry against the Clipper Chip and the electronic encryption policy that announced its availability? Had the government miscalculated the needs of the consumer? Or had the policy wonks misread the degree of trust private businesses had for a government produced and controlled hardware solution to a growing security problem?

**Administration Efforts to Provide Cryptology Policy from 1977-1993**

The issues surrounding the public uses of encryption technology have been causing friction for 20 years, well before the arguments surrounding Clipper It was the publication of work at Stanford University by Whitfield Diffie and Martin Hellman that opened the field of cryptography for academic pursuit absent government funding and also for commercial uses [59] They developed an algorithm that provided efficient transmission of a "public key" and then allowed encrypted communication using "private keys "

At about the same time the Diffie-Hellman algorithm[60] was gaining initial attention, the National Bureau of Standards (NBS)[61] was seeking input to a proposal for the development of a Digital Encryption Standard (DES) The government's intent was to provide the banking and financial industries with a secure method of storing and transmitting data These industries were, of course, closely tied to the government's interest in the domestic economy It was a recognition that money supplies could be manipulated, that financial data were not secure, that led to a more open approach to developing standards

Inevitably, the National Security Agency (NSA) was involved The NSA was the premier U S agency involved in collecting intelligence from across the electronic spectrum during the Cold War They were very good at cryptology It is not surprising, then, that the NSA would be a large

[59] Susan Landau, et al, Codes, Keys, and Conflicts Issues in U S Crypto Policy, Association of Computing Machinery, Inc, June 1994, p 37

[60] Michael H Camilletti, Toward a National Encryption Strategy, National Defense University, unpublished, December 1997, Appendix A "A Cryptology Tutorial"

[61] Now the National Institute of Standards and Technology (NIST)

part of the government's efforts to standardize DES

Businesses and academics were skeptical, however, that a secretive agency such as NSA could have no ulterior motives when developing commercial standards There were fears about "trapdoors" built into programs that would permit clandestine access There were also cases, which many academics feared, of restraint on publication of sensitive research findings [62]

In 1984, President Reagan issued a directive (NSDD 145/14)[63] demanding stricter controls on the protection of nonclassified but sensitive information This included encryption related work Again, business and academics were dismayed What greater motive was lurking behind the front of national security concerns?

The Congress became involved in the mid 1980's, finally passing the Computer Security Act of 1987 Among its provisions was the establishment of civilian control over commercial computer issues This had the effect of moving academic and business related encryption work away from NSA and into the control of the Department of Commerce, National Institute of Standards and Technology (NIST, formerly NBS)

---

A multi year struggle to define what purview remained with the Departments of Defense and State and the Department of Commerce ensued Until this past November (1996), however, decisions about exports were still being made at State after approval by Defense (NSA acting as

---

[62] G A Keyworth, II and David E Colton, Esq , The Computer Revolution, Encryption, and True Threats to National Security, The Progress and Freedom Foundation, Washington, DC, June 1996, p 7

[63] National Security Decision Directive 145/14 established the safeguarding of sensitive but unclassified information that effected National Security

executive for DoD) [64]

As early as 1986, the FBI realized that electronic advances, particularly computing power, would present several challenges to them when investigating crime and developing evidence They initiated a study to examine the potential barriers to electronic evidence collection (wiretaps) that would occur by the spread of encryption technology and by the uses of digital telephone switches

When Senator Joseph Biden introduced Senate Bill S 266, The Comprehensive Counter Terrorist Act, in January 1991, the FBI endorsed the provisions that dealt with encryption controls That bill was withdrawn, but in 1992 the FBI presented a legislative package asking for a wide range of crime prevention and investigation measures that would mitigate the effects of electronic switches in phone systems and restrict the uses of domestic encryption products There were no Senate sponsors for that package

In 1991, NIST was proposing a newer encryption standard, the Digital Signature Standard (DSS) Resistance remained intense from among the business, academic and privacy communities Fundamentally, non government users of encryption did not trust a government developed solution Moreover, they resented restrictions by government on the private development of a secure algorithm

Nonetheless, in April 1993, the White House announced the Clipper Chip A hardware-based encryption tool for business and commercial interests, government offices, and individual uses, it consisted of a sealed silicon chip embedded with a proprietary algorithm developed by NSA (SKIPJACK), a procedure for authorized law enforcement interdiction of message traffic (LEAF),

[64]Dr Clinton Brooks, Special Assistant to the Director, NSA, personal communication

and it featured the DSS [65]

The outcry against Clipper caught the Clinton Administration by surprise No business or private group accepted it Opponents stated that the government's secret algorithm could not be trusted Developers of hardware claimed they needed access to the secret codes in order to market products Academics claimed government was restricting them from using better algorithms Surprisingly, the government was discovered to be still relying on NSA and Defense Department approval for exports of what were supposed to be Commerce Department controlled decisions While that was not directly related to the Clipper program, it was a crisis for an administration that had recently announced and promoted its dedication to the open, global information superhighway Despite the intense scrutiny and debate, Clipper was approved in February 1994 for use and export in commercial devices

The failure of Clipper to gain public acceptance, however, has reduced its use by private, commercial, and business entities AT&T announced a secure telephone using the Clipper Chip in late 1993, but withdrew it from the market following lackluster sales Clipper was quietly withdrawn in 1995 after software-based encryption technologies supplanted hardware solutions in the marketplace

**Analysis of a Policy Challenge**

Policy Development in Government

The Congress reacted in the mid-80's to a growing outcry from business and academic interests that administration policies were stifling the development of commercial products by passing The Computer Security Act of 1987 Among the provisions of this legislation was the

[65] Camilletti, Op cit , Glossary

separation of commercial and business hardware and software encryption applications from those that were strictly military or national security related This provided a clear statement of the intent of Congress They supported the unencumbered development and proliferation of commercial encryption products [66]

Subsequent Congressional actions indicated the clarity of their position that government should avoid controlling the growth and proliferation of electronic goods First, in 1991 when Senator Biden introduced the Comprehensive Counter Terrorism Act, S 266, which was withdrawn for a lack of support. Then in 1992 when no Senator stepped forward to sponsor the FBI's legislative package for electronic crime prevention measures, which would have hampered commercial development efforts And finally, in 1993 when Congress narrowly passed the Digital Telephony Act, which denied the FBI control of domestic encryption technology

The executive branch, for its part, attempted to set policy somewhat independently from the Congress After all, NSA had expertise with encryption and the misuses or challenges it presented For more than 40 years, the ability to encrypt was a virtual government monopoly

Additionally, until the end of the Cold War, it was beyond imagination that enemies (which in practice was every other country of the world) should be provided the technical wherewithal to encrypt their messages using advanced U S technologies Export restrictions made sense So the restrictions against encryption export found in the International Traffic in Arms Regulations (ITAR) and controlled by the joint Defense/State establishment were not recognized by the administration as a violation of the Computer Security Act But it was Even when this was

[66] Lance Hoffman, et al, Cryptology Policy and Technology Trends, Department of Energy, December 1993, p 20

pointed out, the administration acted slowly to clarify its policies

Within the NSA, however, was a group of senior advisors who recognized the inevitability of widespread encryption technology They were aware that the U S lead in developing encryption algorithms was tenuous. They also recognized the approaching point at which simple encryption would overwhelm the computing power available to decrypt files using brute force techniques Using an approach that might be called the "better the devil you know" view, they quietly began to work toward promoting U S encryption exporting worldwide and permitting the widespread commercial development of encryption technologies [67]

Meanwhile, the Department of Justice supported FBI Directors William Sessions and Louis Freeh in their quest for stiff restrictions on encryption export, domestic encryption uses, wiretap authority extended to computer files and e-mail, and law enforcement access to encrypted information via a built-in back door Despite the clear rejections by the Congress of the FBI's wish for stricter, preventive law enforcement measures, Freeh continued to push for tight controls and supported the continued purview of the NSA over encryption developments [68]

---

By April 1993, there was a clearly divided White House that announced the Clipper Chip program At least five different administration entities held one of three competing views about the correct policy Nonetheless, the investment in the Clipper program was substantial and the product was ready

Public Reaction to Policy

---

[67] Cryptography's Role in Securing the Information Society, National Research Council, May 1996

[68] Louis Freeh, testimony to the Senate Committee on the Judiciary, September 1993

Among the public stakeholders in the encryption technology debate there are four more or less separate constituencies First, academics, who wish to conduct unencumbered research and to pursue commercial applications free of government intrusion and restrictions Second, personal freedom advocates, speaking on behalf of constitutionally protected freedoms of speech and against unreasonable searches Third, businesses who require data security and transaction protection within their organization to protect business secrets and to provide data integrity Finally, commercial interests who wish to sell privately developed products in an open market From within these groups emerge two main lines of debate First, the principle of personal freedoms absent government intrusion Second, the adherence to free markets absent government regulation

Regarding the notion of personal freedoms, advocates argue emotionally that government is restricted from infringing a so-called "right to privacy" In practice, however, the Supreme Court has ruled that while a "right to be left alone" is inferred from the Constitution, no prima facie right to privacy is enumerated Historically, the courts hold that government arguments for the protection of national security are valid [69] Additionally, in more recent rulings, courts hold in favor of law enforcement more often than not [70]

As for business interests, the courts are more supportive of the claim that government restrictions hinder fair commercial practices Until a major case is heard by the Supreme Court,

[69] Michael Froomkin, The Metaphor is the Key, University of Pennsylvania Law Review, March 1995, p 795

[70] Ibid, p 853 Froomkin's analysis cites major Supreme Court rulings and analyzes the protections of the 1st, 4th and 5th Amendments to the Constitution thoroughly He concludes that overall, the issue of encryption controls by government is probably valid for the reasons cited

however, such arguments can still be ignored by administration policy makers with impunity

A variety of alliances have been formed from among these related interests They all have in common, however, a resistance to the government's secretive actions regarding Clipper Since selling Clipper chips required a willing group of buyers, the program was risky from the outset for failing to incorporate the needs and desires of the intended market players into the policy

**Conclusions**

How do we assess lessons to be learned from this example of a failed policy? Theory cannot account for a situation in which the views of stakeholders from one interest group are diametrically opposed to those of another group Consensus building, as a means to develop policy might not always work The private and business interests demanding open development and sale of encryption technologies found no compromise with the administration's demand for strict controls

Congress, following a rational actor model of leadership, established a legal basis for compromise to occur between law enforcement, national security, and private interests

Nonetheless, the resulting policy failed Executive branch agencies, particularly the NSA, moved slowly to accommodate the changes in electronic technology that ended their era of control. The FBI, fearing widespread and unbreakable uses of encryption to hide crime, had no choice but to demand strict controls The Department of Commerce, empowered by Congress to establish new approaches to the problem, instead was caught in an organizational trap it needed to rely on NSA technical expertise while it was mandated to operate separately from NSA These effects illustrate the bureaucratic model of policy actions Factions holding strong views can thwart otherwise clearly stated objectives

President Clinton and Vice-president Gore failed to lead Their role was to be the rationale actors They had an opportunity to lead the executive branch agencies and to provide a means to achieve their vision of a public/private partnership in electronic media Instead, they were contradictory in that pursuit At one point they advocated a freely developed electronic infrastructure, while at the same time continuing to hold export restrictions tightly They never achieved a consensus among the agencies they controlled, let alone entered into a dialogue with outside business and private interest groups

For the administration to succeed with a policy against these differing views was a tremendous task Ultimately, the market of non government interests determined the outcome No one bought Clipper Chip equipped devices Indeed the proliferation of software solutions in 1995 and 1996 occurred in part as a response to the failure to succeed with this hardware-based solution Economic theory indicates that market forces will always seek a substitute or a complementary product when barriers to a commodity are high That appears to be the case here When business and private interests could not achieve a policy victory, they abandoned the product itself

Future efforts to control electronic technologies need to recognize this factor Despite government concerns about either national security or domestic law enforcement needs, the market will determine the success or failure of policies regulating development of encryption products As long as government's aims conflict with these market forces, future policies will face the same opposition Building a consensus might not prove possible What is needed is a process that first breaks the organizational and bureaucratic barriers within the administration to achieve compromise among government agencies, leadership to articulate a vision that incorporates the needs of the users, both private and business, and finally, a willingness to accept risk as a new

information-based technology is defined

**NATIONAL DEFENSE UNIVERSITY**

NATIONAL WAR COLLEGE

SCHOOL OF INFORMATION WARFARE AND STRATEGY

# National Security, Law Enforcement, and the Freedom to be Left Alone

*What's Happening in the Encryption Debate?*

---

DECEMBER 19, 1997

MICHAEL H CAMILLETTI/CLASS OF 1998

Directed Research in Information Strategy
Course 5490

FACULTY SEMINAR LEADERS
Dr S Botsai and Mr T Czerwinski

FACULTY ADVISORS
Mr J Stefan and Dr D Kuehl

# National Security, Law Enforcement, and the Freedom to be Left Alone:

*What's Happening in the Encryption Debate?*

A debate played out this summer about the government's right to restrict computing applications that encrypt data and the individual's right to privacy. At stake were business markets for encryption technology overseas, commercial applications to protect company secrets, and personal freedoms. On the government side, the National Security Agency and the Federal Bureau of Investigation demanded strict controls against the exporting of strong encryption products to foreign users and the enactment of domestic controls guaranteeing law enforcement access to encrypted messages and files In the middle was the Clinton Administration, which faced its first challenge from within to the policy for an open, global electronic marketplace Congress tried to referee the debate What happened and how does it affect you?

Encryption is only one part of a larger topic that involves cryptology, the science of encoding

and decoding data Elements of encryption include digital signatures which promote the non repudiation of electronic documents, authenticity certification which promotes the validity of transmitted data, and data security which promotes the protection from unauthorized or unintended view of sensitive information by others

Cryptology, itself, is a small part of the overarching area described as electronic commerce a conceptual framework for all non governmental uses of electronic information transmission and storage personal, private business, and commercial

**Brief History**

***1930-1975***
*Government monopoly on cryptology exists Expense and the scarcity of computing power make the issue unimportant*

***1976-1990***
*Public key cryptography arises Costs go down as processing speed goes up 40 bit export limit arises*

***1991-1994***
*Hardware solutions exist but government controls processes 56 bit and higher export exceptions possible for U S businesses with overseas offices*

***1994-1997***
*Software solutions emerge as platforms provide faster processing power 128 bit domestic solutions and limited, business only, export exceptions are permitted*

Here is a review of the issue as it has developed this year Led by the current administration and several key agencies within the executive branch, the debate has involved major special interest groups, key business leaders, the courts and the Congress

**The Clinton Administration**

The executive branch attempted to set policy when it issued "A Framework for Electronic Commerce," in July 1997 It is a statement of the government's commitment to the Information Age, promoting a tax free and an unregulated, electronic marketplace among the 50 states and overseas Promulgated by the Executive Office of the President through his Information Infrastructure Task Force (IITF), this policy statement was not widely embraced because it included an attempt to force the use of key escrow as a means of providing government access to encrypted

communications, both e-mail and data files

In November, the Presidential Commission for Critical Infrastructure Protection (PCCIP) issued a report enumerating potential threats to national security via electronic attacks against energy, transportation, and communications networks this is known as Information Warfare or IW The commission also endorsed the use of key escrow to provide government access to encrypted files

Simply put, key escrow requires users to deposit the keys to their codes with a third party This provides the FBI investigators ready access to decoding messages when the need arises to investigate potential crimes This idea proved unacceptable to a variety of private and business interests (see sidebar)

The National Security Agency has the most government expertise with encryption technology and the misuses or challenges it presents For more than 40 years, the ability to encrypt data was a virtual government monopoly Additionally, until the end of the Cold War, it

THE DIFFIE-HELLMAN ALGORITHM

Diffie-Hellman key exchange is a public-key technique that takes advantage of the fact that it is easy to compute powers in modular arithmetic, but very difficult to extract logarithms. If $y$ is the $x$th power of $b$, modulo $p$

$$y = b^x \pmod p$$

where b is a suitable base number, then, as in ordinary arithmetic, $x$ is the logarithm of $y$ to the base $b$, modulo $p$

$$x = \log_b y \pmod p$$

Calculation of $y$ from $x$ is easy, but computing $x$ from $y$ is difficult.

In the following illustration using exponential key exchange to establish session keys, the equipment being used to carry out the key distribution is personified as Alice and Bob, just as if the users were doing the computing in their heads The base $b$ is known to both users To initiate communication, Alice chooses a random number $A$ She keeps $A$ secret, but sends

$$b^A \pmod p$$

to Bob Bob in turn chooses a random number, $B$, and sends the corresponding $b^B$ to Alice Both Alice and Bob can now compute

$$b^{AB} \pmod p$$

and use this as their key Bob computes $b^{AB}$ by raising the $b^A$ he obtained from Alice to his secret power $B$

$$(b^A)^B \pmod p = b^{AB} \pmod p$$

Similarly, Alice obtains $(b^B)^A = b^{AB}$ Only Alice and Bob know the secret value $b^{AB}$ There is no known way for anyone who does not know either $A$ or $B$ to compute $b^{AB}$ without first attacking the difficult problem of taking the logarithm of $b^A$ or $b^B$.

If $p$ is a prime about 1,000 bits in length, only about 2,000 multiplications of 1000-bit numbers are required to compute the exponentiation. By contrast, the fastest techniques for taking logarithms in arithmetic modulo $p$ currently demand more than $2^{100}$ (or approximately $10^{30}$) operations Even with today's supercomputers, it would take a billion billion years to perform this many operations

was beyond imagination that enemies (which in practice is every other country of the world) should be provided the technical wherewithal to encrypt their messages using advanced U S technologies So restrictions against encryption export found in the International Traffic in Arms Regulations (ITAR) and controlled by the joint Departments of Defense and State have always been accepted until now

Within the NSA, however, a group of senior advisors recognized the inevitability of widespread encryption technology They were aware that the U S lead in developing encryption algorithms was tenuous They also recognized the approaching point at which simple encryption would overwhelm the computing power available to decrypt files using brute force techniques Using an approach that might be called the "better the devil you know" view, they quietly began to work toward promoting U S encryption exporting worldwide and permitting the widespread commercial development of encryption technologies

As early as 1986, the FBI realized that electronic advances, particularly computing power, would present several challenges to them when investigating crime and developing evidence They initiated a study to examine the potential barriers to electronic evidence collection (wiretaps) that would occur by the spread of encryption technology and by the uses of digital telephone switches

In 1992 the FBI presented a legislative package asking for a wide range of crime prevention and investigation measures that would mitigate the effects of electronic switches in phone systems and restrict the uses of domestic encryption products There were no Senate sponsors for that package

But the Department of Justice supported FBI Director Louis Freeh in his quest for stiff restrictions on encryption export, domestic encryption uses, wiretap authority extended to

computer files and e-mail, and law enforcement access to encrypted information via a built-in back door or key escrow Despite the clear rejections by the Congress of the FBI's wish for stricter, preventive law enforcement measures, Freeh continued to push for tight controls and supported the continued purview of the NSA over encryption developments

**The Public**

Among the public stakeholders in the encryption technology debate there are four more or less separate constituencies First, academics, who wish to conduct unencumbered research and to pursue commercial applications free of government intrusion and restrictions Second, personal freedom advocates, speaking on behalf of constitutionally protected freedoms of speech and against unreasonable searches Third, businesses who require data security and transaction protection within their organization to protect business secrets and to provide data integrity Finally, commercial interests who wish to sell privately developed products in an open market

From within these groups emerge two main lines of debate First, the principle of personal freedoms absent government intrusion Second, the adherence to free markets absent government regulation

Regarding the notion of personal freedoms, advocates argue emotionally that government is restricted from infringing a so-called "right to privacy " In practice, however, the Supreme Court has ruled that while a "right to be left alone" is inferred from the Constitution, no prima facie right to privacy is enumerated Historically, the courts hold that government arguments for the protection of national security are valid Additionally, in more recent rulings, courts hold in favor of law enforcement more often than not

As for business interests, the courts are more supportive of the claim that government

restrictions hinder fair commercial practices Until a major case is heard by the Supreme Court, however, such arguments can still be ignored by administration policy makers with impunity

**The Courts**

There have been three legal challenges mounted against the export controls on encryption technology While decisions in these cases have not been made final, both Congress and the administration are aware of the judicial temper as it is manifest by this issue. Two of the cases, Junger v U S Department of Commerce and Karn v U S Department of State, are still in argument at the trial level

In the third case, Bernstein v U S Department of State, the trial court has found that the export control laws restricting encryption are an unconstitutional prior restraint on speech The court granted an injunction to Professor Bernstein, forbidding the government from prosecuting him for exporting the encryption program he wrote, or any other encryption programs The court specifically stated that it considered granting an injunction against the enforcement of any encryption restrictions The court declined to do this, however, stating that it expected an appeal

---

and wanted the most narrow holding it could devise

The court also held that allowing printed source code to be exported undermined the government's claim that this export control scheme protects any national security Interest The court opined that distinguishing printed from electronic matter probably violates the First Amendment under Reno v ACLU (1997), which held that Internet speech deserves the same

protections as printed speech

**The Congress**

Having watched the administration fumble its policy initiatives and aware that public sentiment demanded some defining action, the Congress debated a variety of bills relative to encryption technology during the summer of 1997

The most talked about and robust bill Congress introduced in 1997, the **Security and Freedom through Encryption (SAFE) Act**, H R 695, was sponsored by Representative Bob Goodlatte of Virginia It has more than 250 cosponsors SAFE emerged from five House committees with three competing versions One amends the bill to say the opposite of its original purpose, another adds provisions for more study The versions of the bill must now be reconciled in the Rules Committee before it can be voted on the House floor

**The Legal Framework**

**The Constitution** empowers the Federal Government with the regulation of commerce, the provision of National Defense, the promotion of public safety, and the protection of personal liberties The government is beset by challenges in administering these often conflicting responsibilities

Policies in one area are found to contradict law, regulation, or other policies from other areas of government. Promoting commerce interferes with protecting public safety national security interests interfere with the global economic interests we need to pursue Protecting liberty raises the risks to innocent persons of violent actions by those who can exploit technology for their own aims

**The National Security Act of 1947** established a framework for fighting the Cold War and provided many of the government restrictions that now encumber electronic commerce The notion that any foreign advantage in computing power would be a disadvantage to the national security prompted a variety of regulatory restrictions that are today embodied in the ITAR and the Department of Commerce's export control rules

**The Computer Security Act of 1987** was passed by Congress to separate the purely military and national security issues regarding computer capacity and technology from the domestic commercial and business interests It established a means to export computer technology worldwide as a means to promote U S competitive advantage In practice, however, the ITAR continued to restrict most export requests for advanced computer applications, including encryption technologies, to weak, non-competitive versions

**The Computer Security Enhancement Act of 1997, H.R. 1903**, was introduced by Representative Sensenbrenner on June 17, 1997 It would amend and update the National

Institute of Standards and Technology Act It is a temporizing measure designed to achieve more study before defining government limits to encryption This bill was passed by the House on September 16 and was referred to the Senate Committee on Commerce

**The Communications Privacy and Consumer Empowerment Act** was introduced by Representative Markey on June 19 This bill would codify existing domestic use policy, permitting unrestricted use of any encryption It would also prohibit the government from requiring key recovery as a criterion for encryption licensing The bill was referred to the House Committee on Commerce

**The Encrypted Communications Privacy Act (ECPA II), S. 376**, was introduced by Senator Leahy on February 27, 1997 ECPA II would prohibit mandatory use of key recovery but would permit law enforcement to obtain keys if recovery were used It would also make it a crime to use cryptography to obstruct justice The bill was referred to the Senate Judiciary Committee, which held hearings on it on July 9

**The Promotion of Commerce Online in the Digital Era (Pro-CODE) Act, S. 377** was introduced by Senator Burns on February 27 Pro-CODE was considered one of the most privacy friendly encryption bills Pro-CODE would have expanded the protections against government intrusion rather than restricted it The Secure Public Networks Act was substituted for Pro-CODE when it came for a vote in the Senate Commerce committee on March 19

**Secure Public Networks Act (SPN), S. 909** is the Clinton Administration's bill. It was sponsored by Senators McCain and Kerrey While its sponsors claim that it would not make key escrow mandatory, SPN would require the use of key recovery systems in order to obtain the "public key certificates" needed to participate in electronic commerce and would require key

recovery for all secure networks built with any federal funds SPN directs the President to negotiate with foreign countries to create a worldwide system for international government access to escrowed keys The bill was referred to the Senate Commerce Committee in March

None of these bills is expected to be passed this session At the time of the December adjournment, Congressional leaders realized that the public debate about this issue was too hot to permit any of the competing bills to move forward

**Outlook 1998 and Beyond**

The status of the encryption technology control issues at the end of 1997 is similar to its status in any preceding year The government insists on control either through proprietary algorithms or key escrow encryption systems There is no movement toward a compromise that would permit greater freedom to export strong encryption products Congress is unlikely to pass any of the competing bills before it this session It will await another cycle of legislative debate before action occurs from that area It will be 1999 or later before a significant case comes before the Supreme Court Meanwhile, District Court cases will shape legal precedent in a variety of ways without impacting the problem significantly

Business is coping with the impact of marketing strong encryption domestically while selling weaker products abroad Whether this will ultimately harm market shares remains to be seen Meanwhile, businesses with overseas offices are being granted limited export permission under the current rules This is being conducted on a case by case basis only and can stop at any time

There are no cases now in which the FBI has been prevented from investigating a crime or prosecuting a suspect for the lack of decrypted data Similarly, there are no cases in which decryption would have prevented a crime from occurring

Finally, no individual has been forced into needlessly losing his privacy over an issue of encryption availability Nor has the government pursued innocent persons via wiretap and electronic surveillance by exploiting weaknesses in cryptologic products

**NATIONAL DEFENSE UNIVERSITY**

NATIONAL WAR COLLEGE

SCHOOL OF INFORMATION WARFARE AND STRATEGY

# The President's Commission for Critical Infrastructure Protection and the National Infrastructure Assurance Agency Proposal

## *Do We Need a New Control Agency?*

DRAFT OUTLINE

February 25, 1998

MICHAEL H CAMILLETTI/CLASS OF 1998

Directed Research in Information Strategy
Course 5490

FACULTY SEMINAR LEADERS
Dr S Botsai and Mr T Czerwinski

FACULTY ADVISORS
Mr J Stefan and Dr D Kuehl

# The President's Commission for Critical Infrastructure Protection and the National Infrastructure Assurance Agency Proposal

## *Do We Need a New Control Agency?*

The President's Commission for Critical Infrastructure Protection (PCCIP) reported in November 1997 a threat to our domestic security from the growing capability of enemies and criminals to disrupt or destroy precious infrastructures including railways, highways, air traffic control systems, energy distribution systems and power plants, computer networks and databases They correctly identified and examined these threats, potential protection from them, and critical priorities to deal with this emerging challenge They recommended a that new agency, the National Infrastructure Assurance Agency (NIAA) be established to handle these tasks But do we really need a new department in government? Isn't downsizing teaching us lessons about how to consolidate functions and seek new efficiencies? Isn't there an agency already prepared to assume these critical missions?

New agency infrastructure arguments for and against and learning curve

Costs and risks

Existing agencies available

The National Security Council

The National Security Agency

The FBI, National Computer Crimes Lab

The Secret Service, U S Department of the Treasury

The Federal Aviation Administration

The National Highway Safety and Transportation Board

The Federal Emergency Management Agency

Timing if threat is high, don't waste time

Proposal for combined agency without new infrastructure

**NATIONAL DEFENSE UNIVERSITY**

NATIONAL WAR COLLEGE

SCHOOL OF INFORMATION WARFARE AND STRATEGY

# A National Strategy for Encryption Technology

DRAFT

---

February 25, 1998

MICHAEL H CAMILLETTI/CLASS OF 1998

Directed Research in Information Strategy
Course 5490

FACULTY SEMINAR LEADERS
Dr S Botsai and Mr T Czerwinski

FACULTY ADVISORS
Mr J Stefan and Dr D Kuehl

# A National Encryption Strategy

## Elements of a National Strategy

If we take the administration at face value, based on the Framework for Electronic Commerce and the statements of both Al Gore and Ira Magaziner, we can envision a future time when unencumbered encryption exists, freely distributed worldwide It enables secure transactions across the Internet, it protects personal and business communications and records Yet it poses no threat to the status quo of law enforcement methods for crime prevention and investigation nor threats to national security

If this is indeed what the administration wishes to achieve, then one approach is to ignore for the moment the barriers now apparent and formulate a strategic model that achieves this goal If we develop such a strategy successfully, then a series of policies should follow that protect ~~individual rights, enhance commerce, and foster public safety domestically and internationally~~ without conflict

The framework for this approach requires us to first ignore the existing barriers First visualize the perfect future state Widespread encryption, free of key recovery (because this is not acceptable to the primary users), yet providing a means for law enforcement and national security elements to continue successfully at their public safety mission How do we reach this goal?

The second step is to identify both the opportunities to achieve this vision and the barriers to its

successful implementation Finally, examining the risks and costs associated with the approach, permits us to realistically evaluate the vision

There is no doubt that national security threats still exist But are they insurmountable? This is no longer the Cold War era when instantaneous decision making is necessary to control events or avert disaster Threats now tend to involve either long term economic goals or short duration terrorist and thug actions, especially those involving weapons of mass destruction The question then is how do we mitigate the need to obtain knowledge of potential threats if encryption is prevalent?

If key recovery is untenable as a means to achieve the vision, the remaining approach is to devote more resources to code analysis and increase the chances for decoding successes Intercepting, analyzing source data, signal data, traffic patterns and message sizes all contribute to the business of understanding encrypted information, yet none of these methods require a plaintext solution Much knowledge can be gained even if encryption is widely used As the NSA official pointed out, " there are things we can do " with source codes

Ultimately, NSA might require a plaintext decryption of a few potentially threatening messages To provide for this, the tools of code breaking need enhancement Brute force methods are deemed impossible once key lengths reach 64 bits But other techniques still remain viable Obtaining the keys, obviously provides a solution Deciphering through direct analysis can succeed Access to the software source code of the program used to encrypt a communication provides additional assistance Our model of unencumbered encryption usage requires a resource shift from maintaining a key recovery based, trusted network to providing more tools and support to existing decoding agencies True, real time decoding is not enhanced by this approach But this

does not differ from the current case when NSA encounters non key escrowed codes This solution still maintains the status quo

The situation is analogous for law enforcement needs First, is an increase in crime likely when encrypted communication deploys widely? This is a debatable point Crime rates will probably follow their historic trends without regard to the uses of encryption Encryption does not enhance committing crime, it only helps to hide crime or to hinder evidence gathering Indeed, the widespread use of encryption can potentially reduce the number of data targets available to the criminal Since encryption that poses such a problem to law enforcement undoubtedly poses a greater problem for criminal elements

A solution for law enforcement, then, is to continue with existing wiretap and surveillance practices Analyze traffic sources, signal data, and other tell tales for appropriate clues, then focus resources on decoding only potentially high value messages Again obtaining the key via court ordered search or subpoena is a first step Next decoding or code analysis is appropriate Again, real time decoding is not enhanced, but is less fatal to law enforcement than is believed (or than the record indicates) Finally, of course, developing other related but unencrypted evidence is always appropriate The essence of this approach is to attack crime with a better use of existing tools and when warranted, to crack codes with additional effort

Resources must be devoted to this approach The National Computer Crime Lab, in cooperation with the National Security Agency and military expertise provide a basis for such an improved capability The PCCIP hinted that such an agency was potentially important (see Article PCCIP and the NIAA)

Absent key recovery schemes, both individuals and businesses are no longer adversaries to

administration policy toward encryption technology Essentially, these interest groups receive what they demand Taxpayers, however, have to foot the bill for new resources devoted to encryption issues This is where a potentially new compromise comes into play

**A Proposal for Encryption Strategy**

If software developers agreed to escrow not the keys, but the source codes of their products and in return received unrestricted freedom to export strong encryption worldwide while pursuing free market strategies for their products, a smaller and less intensive trusted agency would be capable of maintaining the proprietary interests of businesses(similar to patent and copyright protections) while acting as the gatekeepers for national security or law enforcement access to the codes

Separation of interests between law enforcement and trusted agents would be inherent But armed with judicial approval, law enforcement could access the source code from the escrow location and use it to assist in the final code breaking steps, if these became necessary during the pursuit of a potential criminal enterprise While not providing instant decoding capability, NSA experts agree that access to the source code provides, "things we can work with "[71]

Additionally, to fund this approach, a software sales surcharge can be imposed on buyers of encryption products Set at an amount fair to the buyer and capable of funding the trusted system, it might amount to S1 to 5 dollars per sale This could generate up to $250,000,000 00 over time to provide law enforcement with enhanced tools to collect and analyze suspect communications

This approach preserves the freedom of individuals while permitting choice, but with the voluntary recognition that this freedom indeed has a cost It promotes world markets for business

[71] Personal communication with NSA personnel

It addresses law enforcement concerns, albeit to a lesser degree than they demand But approaching the degree to which the documented problem actually exists

Combining competing interests in this way mitigates the arguments while maintaining a reasonable means to prevent catastrophic crime or the erosion of freedoms Policies which result from this over arching strategy achieve the goals identified in the Introduction to this report

**Policy Models**

First, policy for cryptology as part of private communications is supported Individual freedoms from intrusion by government are protected A reasonable expectation of privacy is maintained Choice of the methods, products, and implementation of encryption schemes are entirely open to the individual Costs are reasonably covered by a surcharge on each purchase of encryption capable software or hardware Frequency and degree of use remain matters of individual choice

Second, policy for cryptology as part of business use and electronic commerce will follow an open market model Domestic sales of encryption capable hardware and software are unrestricted A surcharge on each sale can be absorbed by either the manufacturer, the distributor or the purchasers as market forces determine Voluntary disclosure and escrow storage of source code for domestic uses is encouraged but not required Export licenses will be granted for unrestricted worldwide distribution of encryption products subject to the mandatory escrow of the source code Absent an escrow agreement, restricted licenses will be granted for products with capabilities not to exceed 56 bit key lengths Surcharges are payable following the final sale, not at the time of export

Third, policy for cryptology as part of national security will continue as it has for many years The Central Intelligence Agency, the Department of Defense, and the Department of State will

maintain their capabilities to protect national interests Improvements to infrastructure and intelligence activities in the face of increasingly worldwide deployment of encryption technologies will be a matter of budgetary and planning interest The existing capabilities to intercept, analyze, decode and exploit encrypted traffic will be enhanced

Fourth, policies for cryptology as part of law enforcement will enhance the ability of domestic law enforcement to collect information, investigate, and prosecute criminal activities which might use encryption technology or electronic media The Joint National Electronic Crime Lab (JNECL) under the auspices of the Department of Justice and the Department of Defense will exploit domestic intelligence, promote infrastructure protection, and develop crime information The FBI will be the executive agent of the JNECL and will budget and plan for its activities NSA will provide expertise and facilities to complement the needs of the law enforcement community

Fifth, policy for access to source codes, maintained by a trusted agency on behalf of the business community will mirror the policies for wiretap and electronic surveillance embodied in the Omnibus Crime Control and Safe Streets Act of 1968, as amended

## Conclusion

Such a plan can achieve the vision of unencumbered encryption product availability It requires a compromise by businesses, in providing their source codes outside of proprietary business channels, as well as a compromise from law enforcement, to reduce its desire to have unencumbered access to personal communications It preserves civil liberties and protects citizens from potential abuses

It requires leadership and courage to advocate a position that necessarily avoids giving any group everything they wish to achieve It moves the debate away from the potentially paralyzing

impasse in which it now is mired It recognizes the potential ubiquity of new technology to permeate our lives whether we are prepared to adjust to it or not

A Framework for Global Electronic Commerce

Administration Statement on Commercial Encryption Policy

A Framework for Global Electronic Commerce

# A Framework For Global Electronic Commerce

**President William J. Clinton**
**Vice President Albert Gore, Jr.**
**Washington, D.C.**

---

*"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress "*

*Vice President Albert Gore, Jr*

---



---

## BACKGROUND

The Global Information Infrastructure (GII), still in the early stages of its development, is already transforming our world Over the next decade, advances on the GII will affect almost every aspect of daily life -- education, health care, work and leisure activities Disparate populations, once separated by distance and time, will experience these changes as part of a global community

No single force embodies our electronic transformation more than the evolving medium known as the Internet [1] Once a tool reserved for scientific and academic exchange, the Internet has emerged as an appliance of every day life, accessible from almost every point on the planet Students across the world are discovering vast treasure troves of data via the World Wide Web Doctors are utilizing tele-medicine to administer off-site diagnoses to patients in need Citizens of many nations are finding additional outlets for personal and political expression The Internet is being used to reinvent government and reshape our lives and our communities in the process [2]

As the Internet empowers citizens and democratizes societies, it is also changing classic business and economic paradigms New models of commercial interaction are developing as businesses and consumers participate in the electronic marketplace and reap the resultant benefits Entrepreneurs are able to start new businesses more easily, with smaller up-front investment requirements, by accessing the Internet's worldwide network of customers

Internet technology is having a profound effect on the global trade in services World trade involving computer software, entertainment products (motion pictures, videos, games, sound recordings), information services (databases, online newspapers), technical information, product licenses, financial services, and professional services (businesses and technical consulting, accounting, architectural design, legal advice, travel services, etc ) has grown rapidly in the past decade, now accounting for well over $40 billion of U S exports alone [3]

An increasing share of these transactions occurs online The GII has the potential to revolutionize commerce in these and other areas by dramatically lowering transaction costs and facilitating new types of commercial transactions

The Internet will also revolutionize retail and direct marketing Consumers will be able to shop in their homes for a wide variety of products from manufacturers and retailers all over the world They will be able to view these products on their computers or televisions, access information about the products, visualize the way the products may fit together (constructing a room of furniture on their screen, for example), and order and pay for their choice, all from their living rooms

Commerce on the Internet could total tens of billions of dollars by the turn of the century [4] For this potential to be realized fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce Official decision makers must respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining features of the new digital marketplace

Many businesses and consumers are still wary of conducting extensive business over the Internet because of the lack of a predictable legal environment governing transactions This is particularly true for international commercial activity where concerns about enforcement of contracts, liability, intellectual property protection, privacy, security and other matters have caused businesses and consumers to be cautious

As use of the Internet expands, many companies and Internet users are concerned that some governments will impose extensive regulations on the Internet and electronic commerce Potential areas of problematic regulation include taxes and duties, restrictions on the type of information transmitted, control over standards development, licensing requirements and rate regulation of service providers Indeed, signs of these types of commerce-inhibiting actions already are appearing in many nations Preempting these harmful actions before they take root is a strong motivation for the strategy outlined in this paper

Governments can have a profound effect on the growth of commerce on the Internet By their actions, they can facilitate electronic trade or inhibit it Knowing when to act and -- at least as important -- when not to act, will be crucial to the development of electronic commerce [5] This report articulates the Administration's vision for the emergence of the GII as a vibrant global marketplace by suggesting a set of principles, presenting a series of policies, and establishing a road map for international discussions and agreements to facilitate the growth of commerce on the Internet

**PRINCIPLES**

1 ***The private sector should lead.***

Though government played a role in financing the initial development of the Internet, its expansion has been driven primarily by the private sector For electronic commerce to flourish, the private sector must continue to lead Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry

Accordingly, governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them Where government action or intergovernmental agreements are necessary, on taxation for example, private sector participation should be a formal part of the policy making process

2 ***Governments should avoid undue restrictions on electronic commerce.***

Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention Unnecessary regulation of commercial activities will distort development of the electronic marketplace by decreasing the supply and raising the cost of products and services for consumers the world over Business models must evolve rapidly to keep pace with the break-neck speed of change in the technology, government attempts to regulate are likely to be outmoded by the time they are finally enacted, especially to the extent such regulations are technology-specific

Accordingly, governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place via the Internet

3 ***Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.***

In some areas, government agreements may prove necessary to facilitate electronic commerce and protect consumers In these cases, governments should establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation This may involve states as well as national governments Where government intervention is necessary to facilitate electronic commerce, its goal should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution

4 ***Governments should recognize the unique qualities of the Internet.***

The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance These same characteristics pose significant logistical and technological challenges to existing regulatory models, and governments should tailor their policies accordingly

Electronic commerce faces significant challenges where it intersects with existing regulatory schemes We should not assume, for example, that the regulatory frameworks established over the past sixty years for telecommunications, radio and television fit the Internet Regulation should be imposed only as a necessary means to achieve an important goal on which there is a broad consensus Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age

5 ***Electronic Commerce over the Internet should be facilitated on a global basis.***

The Internet is emerging as a global marketplace The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides

**ISSUES**

This paper covers nine areas where international agreements are needed to preserve the Internet as a non-regulatory medium, one in which competition and consumer choice will shape the marketplace Although there are significant areas of overlap, these items can be divided into three main subgroups financial issues, legal issues, and market access issues

**Financial Issues**

- customs and taxation
- electronic payments

**Legal Issues**

- 'Uniform Commercial Code' for electronic commerce
- intellectual property protection
- privacy
- security

**Market Access Issues**

- telecommunications infrastructure and information technology
- content
- technical standards

## I. Financial Issues

### 1. CUSTOMS AND TAXATION

For over 50 years, nations have negotiated tariff reductions because they have recognized that the economies and citizens of all nations benefit from freer trade Given this recognition, and because the Internet is truly a global medium, it makes little sense to introduce tariffs on goods and services delivered over the Internet

Further, the Internet lacks the clear and fixed geographic lines of transit that historically have characterized the physical trade of goods Thus, while it remains possible to administer tariffs for products ordered over the Internet but ultimately delivered via surface or air transport, the structure of the Internet makes it difficult to do so when the product or service is delivered electronically

Nevertheless, many nations are looking for new sources of revenue, and may seek to levy tariffs on global electronic commerce

Therefore, the United States will advocate in the World Trade Organization (WTO) and other appropriate international fora that the Internet be declared a tariff-free environment whenever it is used to deliver products or services This principle should be established quickly before nations impose tariffs and before vested interests form to protect those tariffs

In addition, the United States believes that no new taxes should be imposed on Internet commerce The taxation of commerce conducted over the Internet should be consistent with the established principles of international taxation, should avoid inconsistent national tax jurisdictions and double taxation, and should be simple to administer and easy to understand

Any taxation of Internet sales should follow these principles

- It should neither distort nor hinder commerce No tax system should discriminate among types of commerce, nor should it create incentives that will change the nature or location of transactions

- The system should be simple and transparent It should be capable of capturing the overwhelming majority of appropriate revenues, be easy to implement, and minimize burdensome record keeping and costs for all parties

- The system should be able to accommodate tax systems used by the United States and our international partners today

Wherever feasible, we should look to existing taxation concepts and principles to achieve these goals

Any such taxation system will have to accomplish these goals in the context of the Internet's special characteristics -- the potential anonymity of buyer and seller, the capacity for multiple small transactions, and the difficulty of associating online activities with physically defined locations

To achieve global consensus on this approach, the United States, through the Treasury Department, is participating in discussions on the taxation of electronic commerce through the Organization for Economic Cooperation and Development (OECD), the primary forum for cooperation in international taxation

The Administration is also concerned about possible moves by state and local tax authorities to target electronic commerce and Internet access The uncertainties associated with such taxes and the inconsistencies among them could stifle the development of Internet commerce

The Administration believes that the same broad principles applicable to international taxation, such as not hindering the growth of electronic commerce and neutrality between conventional and electronic commerce, should be applied to subfederal taxation No new taxes should be applied to electronic commerce, and states should coordinate their allocation of income derived from electronic commerce Of course, implementation of these principles may differ at the subfederal level where indirect taxation plays a larger role

Before any further action is taken, states and local governments should cooperate to develop a uniform, simple approach to the taxation of electronic commerce, based on existing principles of taxation where feasible

## 2. ELECTRONIC PAYMENT SYSTEMS

New technology has made it possible to pay for goods and services over the Internet Some of the methods would link existing electronic banking and payment systems, including credit and debit card networks, with new retail interfaces via the Internet "Electronic money," based on stored-value, smart card, or other technologies, is also under development Substantial private sector investment and competition is spurring an intense period of innovation that should benefit consumers and businesses wishing to engage in global electronic commerce

At this early stage in the development of electronic payment systems, the commercial and technological environment is changing rapidly It would be hard to develop policy that is both timely and appropriate For these reasons, inflexible and highly prescriptive regulations and rules are inappropriate and potentially harmful Rather, in the near term, case-by-case monitoring of electronic payment experiments is preferred

From a longer term perspective, however, the marketplace and industry self-regulation alone may not fully address all issues For example, government action may be necessary to ensure the safety and soundness of electronic payment systems, to protect consumers, or to respond to important law enforcement objectives

The United States, through the Department of the Treasury, is working with other governments in international fora to study the global implications of emerging electronic payment systems A number of organizations are already working on important aspects of electronic banking and payments [6] Their analyses will contribute to a better understanding of how electronic payment systems will affect global commerce and banking

The Economic Communique issued at the Lyon Summit by the G-7 Heads of State called for a cooperative study of the implications of new, sophisticated retail electronic payment systems In response, the G-10 deputies formed a Working Party, with representation from finance ministries and central banks (in consultation with law enforcement authorities) The Working Party is chaired by a representative from the U S Treasury Department, and tasked to produce a report that identifies common policy objectives among the G-10 countries and analyzes the national approaches to electronic commerce taken to date

As electronic payment systems develop, governments should work closely with the private sector to inform policy development, and ensure that governmental activities flexibly accommodate the needs of the emerging marketplace

## II. Legal Issues

### 3. 'UNIFORM COMMERCIAL CODE' FOR ELECTRONIC COMMERCE

In general, parties should be able to do business with each other on the Internet under whatever terms and conditions they agree upon

Private enterprise and free markets have typically flourished, however, where there are predictable and widely accepted legal environments supporting commercial transactions To encourage electronic commerce, the U S government should support the development of both a domestic and global uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide Fully informed buyers and sellers could voluntarily agree to form a contract subject to this uniform legal framework, just as parties currently choose the body of law that will be used to interpret their contract

Participants in the marketplace should define and articulate most of the rules that will govern electronic commerce To enable private entities to perform this task and to fulfill their roles adequately, governments should encourage the development of simple and predictable domestic and international rules and norms that will serve as the legal foundation for commercial activities in cyberspace

In the United States, every state government has adopted the Uniform Commercial Code (UCC), a codification of substantial portions of commercial law The National Conference of Commissioners of Uniform State Law (NCCUSL) and the American Law Institute, domestic sponsors of the UCC, already are working to adapt the UCC to cyberspace Private sector

organizations, including the American Bar Association (ABA) along with other interest groups, are participants in this process Work is also ongoing on a proposed electronic contracting and records act for transactions not covered by the UCC The Administration supports the prompt consideration of these proposals, and the adoption of uniform legislation by all states Of course, any such legislation will be designed to accommodate ongoing and possible future global initiatives

Internationally, the United Nations Commission on International Trade Law (UNCITRAL) has completed work on a model law that supports the commercial use of international contracts in electronic commerce This model law establishes rules and norms that validate and recognize contracts formed through electronic means, sets default rules for contract formation and governance of electronic contract performance, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings

The United States Government supports the adoption of principles along these lines by all nations as a start to defining an international set of uniform commercial principles for electronic commerce We urge UNCITRAL, other appropriate international bodies, bar associations, and other private sector groups to continue their work in this area

The following principles should, to the extent possible, guide the drafting of rules governing global electronic commerce

- parties should be free to order the contractual relationship between themselves as they see fit,
- rules should be technology-neutral (i e , the rules should neither require nor assume a particular technology) and forward looking (i e , the rules should not hinder the use or development of technologies in the future),
- existing rules should be modified and new rules should be adopted only as necessary or substantially desirable to support the use of electronic technologies, and
- the process should involve the high-tech commercial sector as well as businesses that have not yet moved online

With these principles in mind, UNCITRAL, UNIDROIT, and the International Chamber of Commerce (ICC), and others should develop additional model provisions and uniform fundamental principles designed to eliminate administrative and regulatory barriers and to facilitate electronic commerce by

- encouraging governmental recognition, acceptance and facilitation of electronic communications (i e , contracts, notarized documents, etc ),
- encouraging consistent international rules to support the acceptance of electronic signatures and other authentication procedures, and
- promoting the development of adequate, efficient, and effective alternate dispute resolution mechanisms for global commercial transactions

The expansion of global electronic commerce also depends upon the participants' ability to

achieve a reasonable degree of certainty regarding their exposure to liability for any damage or injury that might result from their actions Inconsistent local tort laws, coupled with uncertainties regarding jurisdiction, could substantially increase litigation and create unnecessary costs that ultimately will be born by consumers The U S should work closely with other nations to clarify applicable jurisdictional rules and to generally favor and enforce contract provisions that allow parties to select substantive rules governing liability

Finally, the development of global electronic commerce provides an opportunity to create legal rules that allow business and consumers to take advantage of new technology to streamline and automate functions now accomplished manually For example, consideration should be given to establishing electronic registries

The Departments of Commerce and State will continue to organize U S participation in these areas with a goal of achieving substantive international agreement on model law within the next two years NCCUSL and the American Law Institute, working with the American Bar Association and other interested groups, are urged to continue their work to develop complementary domestic and international efforts

## 4. INTELLECTUAL PROPERTY PROTECTION

Commerce on the Internet often will involve the sale and licensing of intellectual property To promote this commerce, sellers must know that their intellectual property will not be stolen and buyers must know that they are obtaining authentic products

International agreements that establish clear and effective copyright, patent, and trademark protection are therefore necessary to prevent piracy and fraud While technology, such as encryption, can help combat piracy, an adequate and effective legal framework also is necessary to deter fraud and the theft of intellectual property, and to provide effective legal recourse when these crimes occur Increased public education about intellectual property in the information age will also contribute to the successful implementation and growth of the GII

### Copyrights

There are several treaties that establish international norms for the protection of copyrights, most notably the Berne Convention for the Protection of Literary and Artistic Works These treaties link nearly all major trading nations and provide them with a means of protecting, under their own laws, each other's copyrighted works and sound recordings

In December 1996, the World Intellectual Property Organization (WIPO) updated the Berne Convention and provided new protection for performers and producers of sound recordings by adopting two new treaties The two treaties -- the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty -- will greatly facilitate the commercial applications of online digital communications over the GII

Both treaties include provisions relating to technological protection, copyright management information, and the right of communication to the public, all of which are indispensable for an efficient exercise of rights in the digital environment The U S Government recognizes private sector efforts to develop international and domestic standards in these areas The Administration understands the sensitivities associated with copyright management information and technological

protection measures, and is working to tailor implementing legislation accordingly

Both treaties also contain provisions that permit nations to provide for exceptions to rights in certain cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author (*e g* , "fair use") These provisions permit members to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention These provisions permit members to devise new exceptions and limitations that are appropriate in the digital network environment, but neither reduce nor extend the scope of applicability of the limitations and exceptions permitted by the Berne Convention

The Administration is drafting legislation to implement the new WIPO treaties, and looks forward to working with the Senate on their ratification

The two new WIPO treaties do not address issues of online service provider liability, leaving them to be determined by domestic legislation The Administration looks forward to working with Congress as these issues are addressed and supports efforts to achieve an equitable and balanced solution that is agreeable to interested parties and consistent with international copyright obligations

The adoption of the two new WIPO treaties represents the attainment of one of the Administration's significant intellectual property objectives The U S Government will continue to work for appropriate copyright protection for works disseminated electronically The Administration's copyright-related objectives will include

- encouraging countries to fully and immediately implement the obligations contained in the Agreement on Trade-Related Aspects of Intellectual Property (TRIPS),
- seeking immediate U S ratification and deposit of the instruments of accession to the two new WIPO treaties and implementation of the obligations in these treaties in a balanced and appropriate way as soon as possible,
- encouraging other countries to join the two new WIPO treaties and to implement fully the treaty obligations as soon as possible, and
- ensuring that U S trading partners establish laws and regulations that provide adequate and effective protection for copyrighted works, including motion pictures, computer software, and sound recordings, disseminated via the GII, and that these laws and regulations are fully implemented and actively enforced

The United States will pursue these international objectives through bilateral discussions and multilateral discussions at WIPO and other appropriate fora and will encourage private sector participation in these discussions

***Sui Generis* Protection of Databases**

The December 1996 WIPO Conference in Geneva did not take up a proposed treaty to protect the non-original elements of databases Instead, the Conference called for a meeting, subsequently held, to discuss preliminary steps to study proposals to establish *sui generis* database protection

Based on the brief discussion of *sui generis* database protection that took place before and during the Diplomatic Conference, it is clear that more discussion of the need for and the nature of such protection is necessary domestically and internationally

The Administration will seek additional input from, among others, the scientific, library, and academic communities and the commercial sector, in order to develop U S policy with respect to *sui generis* database protection

**Patents**

Development of the GII will both depend upon and stimulate innovation in many fields of technology, including computer software, computer hardware, and telecommunications An effectively functioning patent system that encourages and protects patentable innovations in these fields is important for the overall success of commerce over the Internet Consistent with this objective, the U S Patent and Trademark Office (PTO) will (1) significantly enhance its collaboration with the private sector to assemble a larger, more complete collection of prior art (both patent and non-patent publications), and provide its patent examiners better access to prior art in GII-related technologies, (2) train its patent examiners in GII-related technologies to raise and maintain their level of technical expertise, and (3) support legislative proposals for early publication of pending patent applications, particularly in areas involving fast moving technology

To create a reliable environment for electronic commerce, patent agreements should

- prohibit member countries from authorizing parties to exploit patented inventions related to the GII without the patent owner's authority (i e , disapproval of compulsory licensing of GII-related technology except to remedy a practice determined after judicial or administrative process to be anti-competitive),
- require member countries to provide adequate and effective protection for patentable subject matter important to the development and success of the GII, and
- establish international standards for determining the validity of a patent claim

The United States will pursue these objectives internationally Officials of the European, Japanese, and United States Patent Offices meet, for example, each year to foster cooperation on patent-related issues The United States will recommend at the next meeting that a special committee be established within the next year to make recommendations on GII-related patent issues

In a separate venue, one hundred countries and international intergovernmental organizations participate as members of WIPO's permanent committee on industrial property information (PCIPI) The United States will attempt to establish a working group of this organization to address GII-related patent issues

**Trademark and Domain Names**

Trademark rights are national in scope and conflicts may arise where the same or similar trademarks for similar goods or services are owned by different parties in different countries Countries may also apply different standards for determining infringement

Conflicts have arisen on the GII where third parties have registered Internet domain names that are the same as, or similar to, registered or common law trademarks An Internet domain name functions as a source identifier on the Internet Ordinarily, source identifiers, like addresses, are not protected intellectual property (i e , a trademark) *per se* The use of domain names as source identifiers has burgeoned, however, and courts have begun to attribute intellectual property rights to them, while recognizing that misuse of a domain name could significantly infringe, dilute, and weaken valuable trademark rights

To date, conflicts between trademark rights and domain names have been resolved through negotiations and/or litigation It may be possible to create a contractually based self- regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis without the need to litigate This could create a more stable business environment on the Internet Accordingly, the United States will support efforts already underway to create domestic and international fora for discussion of Internet-related trademark issues The Administration also plans to seek public input on the resolution of trademark disputes in the context of domain names

Governance of the domain name system (DNS) raises other important issues unrelated to intellectual property The Administration supports private efforts to address Internet governance issues including those related to domain names and has formed an interagency working group under the leadership of the Department of Commerce to study DNS issues The working group will review various DNS proposals, consulting with interested private sector, consumer, professional, congressional and state government and international groups The group will consider, in light of public input, (1) what contribution government might make, if any, to the development of a global competitive, market-based system to register Internet domain names, and (2) how best to foster bottom-up governance of the Internet

**5. PRIVACY**

Americans treasure privacy, linking it to our concept of personal freedom and well- being Unfortunately, the GII's great promise -- that it facilitates the collection, re-use, and instantaneous transmission of information -- can, if not managed carefully, diminish personal privacy It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business

At the same time, fundamental and cherished principles like the First Amendment, which is an important hallmark of American democracy, protect the free flow of information Commerce on the GII will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information

In June of 1995, the Privacy Working Group of the United States government Information Infrastructure Task Force (IITF) issued a report entitled, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE Principles for Providing and Using Personal Information The report recommends a set of principles (the "Privacy Principles") to govern the collection, processing, storage, and re-use of personal data in the information age

These Privacy Principles, which build on the Organization for Economic Cooperation and Development's GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER DATA FLOW OF PERSONAL DATA and incorporate principles of fair

information practices, rest on the fundamental precepts of awareness and choice

- Data-gatherers should inform consumers what information they are collecting, and how they intend to use such data, and

- Data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information

Disclosure by data-gatherers is designed to stimulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge about why information is being collected, what the information will be used for, what steps will be taken to protect that information, the consequences of providing or withholding information, and any rights of redress that they may have Such disclosure will enable consumers to make better judgments about the levels of privacy available and their willingness to participate

In addition, the Privacy Principles identify three values to govern the way in which personal information is acquired, disclosed and used online -- information privacy, information integrity, and information quality First, an individual's reasonable expectation of privacy regarding access to and use of, his or her personal information should be assured Second, personal information should not be improperly altered or destroyed And, third, personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and used

Under these principles, consumers are entitled to redress if they are harmed by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information

In April, 1997, the Information Policy Committee of the IITF issued a draft paper entitled Options For Promoting Privacy on the National Information Infrastructure The paper surveys information practices in the United States and solicits public comment on the best way to implement the Privacy Principles The IITF goal is to find a way to balance the competing values of personal privacy and the free flow of information in a digital democratic society

Meanwhile, other federal agencies have studied privacy issues in the context of specific industry sectors In October 1995, for example, the National Telecommunications and Information Administration (NTIA) issued a report entitled Privacy and the NII Safeguarding Telecommunications-Related Personal Information It explores the application of the Privacy Principles in the context of telecommunications and online services and advocates a voluntary framework based on notice and consent [7] On January 6, 1997, the FTC issued a staff report entitled Public Workshop on Consumer Privacy on the Global Information Infrastructure The report, which focuses on the direct marketing and advertising industries, concludes that notice, choice, security, and access are recognized as necessary elements of fair information practices online In June of 1997, the FTC held four days of hearings on technology tools and industry self-regulation regimes designed to enhance personal privacy on the Internet

The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution

The Administration also anticipates that technology will offer solutions to many privacy concerns in the online environment, including the appropriate use of anonymity If privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online

The Administration is particularly concerned about the use of information gathered from children, who may lack the cognitive ability to recognize and appreciate privacy concerns Parents should be able to choose whether or not personally identifiable information is collected from or about their children We urge industry, consumer, and child-advocacy groups working together to use a mix of technology, self-regulation, and education to provide solutions to the particular dangers arising in this area and to facilitate parental choice This problem warrants prompt attention Otherwise, government action may be required

Privacy concerns are being raised in many countries around the world, and some countries have enacted laws, implemented industry self-regulation, or instituted administrative solutions designed to safeguard their citizens' privacy Disparate policies could emerge that might disrupt transborder data flows For example, the European Union (EU) has adopted a Directive that prohibits the transfer of personal data to countries that, in its view, do not extend adequate privacy protection to EU citizens

To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled

The United States will continue policy discussions with the EU nations and the European Commission to increase understanding about the U S approach to privacy and to assure that the criteria they use for evaluating adequacy are sufficiently flexible to accommodate our approach These discussions are led by the Department of Commerce, through NTIA, and the State Department, and include the Executive Office of the President, the Treasury Department, the Federal Trade Commission (FTC) and other relevant federal agencies NTIA is also working with the private sector to assess the impact that the implementation of the EU Directive could have on the United States

The United States also will enter into a dialogue with trading partners on these issues through existing bilateral fora as well as through regional fora such as the Asia Pacific Economic Cooperation (APEC) forum, the Summit of the Americas, the North American Free Trade Agreement (NAFTA), and the Inter-American Telecommunications Commission (CITEL) of the Organization of American States, and broader multilateral organizations

The Administration considers data protection critically important We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy

**6. SECURITY**

The GII must be secure and reliable If Internet users do not have confidence that their communications and data are safe from unauthorized access or modification, they will be unlikely to use the Internet on a routine basis for commerce

A secure GII requires

1 secure and reliable telecommunications networks,

2 effective means for protecting the information systems attached to those networks,

3 effective means for authenticating and ensuring confidentiality of electronic information to protect data from unauthorized use, and

4 well trained GII users who understand how to protect their systems and their data

There is no single "magic" technology or technique that can ensure that the GII will be secure and reliable Accomplishing that goal requires a range of technologies (encryption, authentication, password controls, firewalls, etc ) and effective, consistent use of those technologies, all supported globally by trustworthy key and security management infrastructures

Of particular importance is the development of trusted certification services that support the digital signatures that will permit users to know whom they are communicating with on the Internet Both signatures and confidentiality rely on the use of cryptographic keys To promote the growth of a trusted electronic commerce environment, the Administration is encouraging the development of a voluntary, market-driven key management infrastructure that will support authentication, integrity, and confidentiality

Encryption products protect the confidentiality of stored data and electronic communications by making them unreadable without a decryption key But strong encryption is a double-edged sword Law abiding citizens can use strong encryption to protect their trade secrets and personal records But those trade secrets and personal records could be lost forever if the decrypt key is lost Depending upon the value of the information, the loss could be quite substantial Encryption can also be used by criminals and terrorists to reduce law enforcement capabilities to read their communications Key recovery based encryption can help address some of these issues

In promoting robust security needed for electronic commerce, the Administration has already taken steps that will enable trust in encryption and provide the safeguards that users and society will need The Administration, in partnership with industry, is taking steps to promote the development of market-driven standards, public-key management infrastructure services and key recoverable encryption products Additionally, the Administration has liberalized export controls for commercial encryption products while protecting public safety and national security interests

The Administration is also working with Congress to ensure legislation is enacted that would facilitate development of voluntary key management infrastructures and would govern the release of recovery information to law enforcement officials pursuant to lawful authority

The U S government will work internationally to promote development of market- driven key management infrastructure with key recovery Specifically, the U S has worked closely within the

OECD to develop international guidelines for encryption policies and will continue to promote the development of policies to provide a predictable and secure environment for global electronic commerce

## III. Market Access Issues

### 7. TELECOMMUNICATIONS INFRASTRUCTURE AND INFORMATION TECHNOLOGY

Global electronic commerce depends upon a modern, seamless, global telecommunications network and upon the computers and "information appliances" that connect to it [8] Unfortunately, in too many countries, telecommunications policies are hindering the development of advanced digital networks Customers find that telecommunications services often are too expensive, bandwidth is too limited, and services are unavailable or unreliable Likewise, many countries maintain trade barriers to imported information technology, making it hard for both merchants and customers to purchase the computers and information systems they need to participate in electronic commerce

In order to spur the removal of barriers, in March 1994, Vice President Gore spoke to the World Telecommunications Development Conference in Buenos Aires He articulated several principles that the U S believes should be the foundation for government policy, including

1 encouraging private sector investment by privatizing government-controlled telecommunications companies,

2 promoting and preserving competition by introducing competition to monopoly phone markets, ensuring interconnection at fair prices, opening markets to foreign investment, and enforcing anti-trust safeguards,

3 guaranteeing open access to networks on a non-discriminatory basis, so that GII users have access to the broadest range of information and services, and

4 implementing, by an independent regulator, pro-competitive and flexible regulation that keeps pace with technological development [9]

Domestically, the Administration recognizes that there are various constraints in the present network that may impede the evolution of services requiring higher bandwidth Administration initiatives include Internet II, or Next Generation Internet In addition, the FCC has undertaken several initiatives designed to stimulate bandwidth expansion, especially to residential and small/home office customers

The goal of the United States will be to ensure that online service providers can reach end-users on reasonable and nondiscriminatory terms and conditions Genuine market opening will lead to increased competition, improved telecommunications infrastructures, more customer choice, lower prices and increased and improved services

Areas of concern include

- Leased lines Data networks of most online service providers are constructed with leased lines that must be obtained from national telephone companies, often monopolies or governmental

entities In the absence of effective competition, telephone companies may impose artificially inflated leased line prices and usage restrictions that impede the provision of service by online service providers

- Local loops pricing To reach their subscribers, online service providers often have no choice but to purchase local exchange services from monopoly or government-owned telephone companies These services also are often priced at excessive rates, inflating the cost of data services to customers

- Interconnection and unbundling Online service providers must be able to interconnect with the networks of incumbent telecommunication companies so that information can pass seamlessly between all users of the network Monopolies or dominant telephone companies often price interconnection well above cost, and refuse to interconnect because of alleged concerns about "network compatibility" or "absence of need for other providers "

- Attaching equipment to the network Over the years, some telecommunication providers have used their monopoly power to restrict the connection of communication or technology devices to the network Even when the monopoly has been broken, a host of unnecessary burdensome "type acceptance" practices have been used to retard competition and make it difficult for consumers to connect

- Internet voice and multimedia Officials of some nations claim that "real time" services provided over the Internet are "like services" to traditionally regulated voice telephony and broadcasting, and therefore should be subject to the same regulatory restrictions that apply to those traditional services In some countries, these providers must be licensed, as a way to control both the carriage and content offered Such an approach could hinder the development of new technologies and new services

In addition, countries have different levels of telecommunications infrastructure development, which may hinder the global provision and use of some Internet-based services The Administration believes that the introduction of policies promoting foreign investment, competition, regulatory flexibility and open access will support infrastructure development and the creation of more data-friendly networks

To address these issues, the Administration successfully concluded the WTO Basic Telecommunications negotiations, which will ensure global competition in the provision of basic telecommunication services and will address the many underlying issues affecting online service providers During those negotiations, the U S succeeded in ensuring that new regulatory burdens would not be imposed upon online service providers that would stifle the deployment of new technologies and services

As the WTO Agreement is implemented, the Administration will seek to ensure that new rules of competition in the global communications marketplace will be technology neutral and will not hinder the development of electronic commerce In particular, rules for licensing new technologies and new services must be sufficiently flexible to accommodate the changing needs of consumers while allowing governments to protect important public interest objectives like universal service In this context, rules to promote such public interest objectives should not fall disproportionately on any one segment of the telecommunications industry or on new entrants

The Administration will also seek effective implementation of the Information Technology Agreement concluded by the members of the WTO in March 1997, which is designed to remove tariffs on almost all types of information technology Building on this success, and with the encouragement of U S companies, the administration is developing plans for ITA II, in which it will to seek to remove remaining tariffs on, and existing non-tariff barriers to, information technology goods and services In addition, the Administration is committed to finding other ways to streamline requirements to demonstrate product conformity, including through "Mutual Recognition Agreements" (MRAS) that can eliminate the need for a single product to be certified by different standards laboratories across national borders

Bilateral exchanges with individual foreign governments, regional fora such as APEC and CITEL, and multilateral fora such as the OECD and ITU, and various other fora (*i e* international alliances of private businesses, the International Organization of Standardization [ISO], the International Electrotechnical Commission [IEC]), also will be used for international discussions on telecommunication-related Internet issues and removing trade barriers that inhibit the export of information technology These issues include the terms and conditions governing the exchange of online traffic, addressing, and reliability In all fora, U S Government positions that might influence Internet pricing, service delivery options or technical standards will reflect the principles established in this paper and U S Government representatives will survey the work of their study groups to ensure that this is the case

In addition, many Internet governance issues will best be dealt with by means of private, open standards processes and contracts involving participants from both government and the private sector The U S government will support industry initiatives aimed at achieving the important goals outlined in this paper

## 8. CONTENT

The U S government supports the broadest possible free flow of information across international borders This includes most informational material now accessible and transmitted through the Internet, including through World Wide Web pages, news and other information services, virtual shopping malls, and entertainment features, such as audio and video products, and the arts This principle extends to information created by commercial enterprises as well as by schools, libraries, governments and other nonprofit entities

In contrast to traditional broadcast media, the Internet promises users greater opportunity to shield themselves and their children from content they deem offensive or inappropriate New technology, for example, may enable parents to block their children's access to sensitive information or confine their children to pre-approved websites

To the extent, then, that effective filtering technology becomes available, content regulations traditionally imposed on radio and television would not need to be applied to the Internet In fact, unnecessary regulation could cripple the growth and diversity of the Internet

The Administration therefore supports industry self-regulation, adoption of competing ratings systems, and development of easy-to-use technical solutions (*e g* , filtering technologies and age verification systems) to assist in screening information online

There are four priority areas of concern

- Regulation of content Companies wishing to do business over the Internet, and to provide access to the Internet (including U S online service providers with foreign affiliates or joint ventures) are concerned about liability based on the different policies of every country through which their information may travel

  Countries that are considering or have adopted laws to restrict access to certain types of content through the Internet emphasize different concerns as a result of cultural, social, and political difference These different laws can impede electronic commerce in the global environment

  The Administration is concerned about Internet regulation of this sort, and will develop an informal dialogue with key trading partners on public policy issues such as hate speech, violence, sedition, pornography and other content to ensure that differences in national regulation, especially those undertaken to foster cultural identity, do not serve as disguised trade barriers

- Foreign content quotas Some countries currently require that a specific proportion of traditional broadcast transmission time be devoted to "domestically produced" content Problems could arise on the Internet if the definition of "broadcasting" is changed to extend these current regulations to "new services " Countries also might decide to regulate Internet content and establish restrictions under administrative authority, rather than under broadcast regulatory structures

  The Administration will pursue a dialogue with other nations on how to promote content diversity, including cultural and linguistic diversity, without limiting content These discussions could consider promotion of cultural identity through subsidy programs that rely solely on general tax revenues and that are implemented in a nondiscriminatory manner

- Regulation of advertising Advertising will allow the new interactive media to offer more affordable products and services to a wider, global audience Some countries stringently restrict the language, amount, frequency, duration, and type of tele-shopping and advertising spots used by advertisers In principle, the United States does not favor such regulations While recognizing legitimate cultural and social concerns, these concerns should not be invoked to justify unnecessarily burdensome regulation of the Internet

  There are laws in many countries around the world that require support for advertising claims Advertising industry self-regulation also exists in many countries around the globe Truthful and accurate advertising should be the cornerstone of advertising on all media, including the Internet

  A strong body of cognitive and behavioral research demonstrates that children are particularly vulnerable to advertising As a result, the U S has well established rules (self- regulatory and otherwise) for protecting children from certain harmful advertising practices The Administration will work with industry and childrens advocates to ensure that these protections are translated to and implemented appropriately in the online media environment

The rules of the "country-of-origin" should serve as the basis for controlling Internet advertising to alleviate national legislative roadblocks and trade barriers

- Regulation to prevent fraud Recently, there have been a number of cases where fraudulent information on companies and their stocks, and phony investment schemes have been broadcast on the Internet The appropriate federal agencies (i e , Federal Trade Commission and the Securities and Exchange Commission) are determining whether new regulations are needed to prevent fraud over the Internet

In order to realize the commercial and cultural potential of the Internet, consumers must have confidence that the goods and services offered are fairly represented, that they will get what they pay for, and that recourse or redress will be available if they do not This is an area where government action is appropriate

The Administration will explore opportunities for international cooperation to protect consumers and to prosecute false, deceptive, and fraudulent commercial practices in cyberspace

Federal agencies such as the Department of State, U S Trade Representative (USTR), the Commerce Department (NTIA), the FTC, the Office of Consumer Affairs and others have already engaged in efforts to promote such positions, through both bilateral and multilateral channels, including through the OECD, the G-7 Information Society and Development Conference, the Latin American Telecommunications Summits, and the Summit of the Americas process, as well as APEC Telecommunications Ministerials All agencies participating in such fora will focus on pragmatic solutions based upon the principles in this paper to issues related to content control

## 9. TECHNICAL STANDARDS

Standards are critical to the long term commercial success of the Internet as they can allow products and services from different vendors to work together They also encourage competition and reduce uncertainty in the global marketplace Premature standardization, however, can "lock in" outdated technology Standards also can be employed as *de facto* non-tariff trade barriers, to "lock out" non-indigenous businesses from a particular national market

The United States believes that the marketplace, not governments, should determine technical standards and other mechanisms for interoperability Technology is moving rapidly and government attempts to establish technical standards to govern the Internet would only risk inhibiting technological innovation The United States considers it unwise and unnecessary for governments to mandate standards for electronic commerce Rather, we urge industry driven multilateral fora to consider technical standards in this area

To ensure the growth of global electronic commerce over the Internet, standards will be needed to assure reliability, interoperability, ease of use and scalability in areas such as

- electronic payments,

- security (confidentiality, authentication, data integrity, access control, non-repudiation),

- security services infrastructure (*e g* , public key certificate authorities),
- electronic copyright management systems,
- video and data-conferencing,
- high-speed network technologies (*e g* , Asynchronous Transfer Mode, Synchronous Digital Hierarchy), and
- digital object and data interchange

There need not be one standard for every product or service associated with the GII, and technical standards need not be mandated In some cases, multiple standards will compete for marketplace acceptance In other cases, different standards will be used in different circumstances

The prevalence of voluntary standards on the Internet, and the medium's consensus- based process of standards development and acceptance are stimulating its rapid growth These standards flourish because of a non-bureaucratic system of development managed by technical practitioners working through various organizations These organizations require demonstrated deployment of systems incorporating a given standard prior to formal acceptance, but the process facilitates rapid deployment of standards and can accommodate evolving standards as well Only a handful of countries allow private sector standards development, most rely on government- mandated solutions, causing these nations to fall behind the technological cutting edge and creating non-tariff trade barriers

Numerous private sector bodies have contributed to the process of developing voluntary standards that promote interoperability The United States has encouraged the development of voluntary standards through private standards organizations, consortia, testbeds and R&D activities [10] The U S government also has adopted a set of principles to promote acceptance of domestic and international voluntary standards

While no formal government-sponsored negotiations are called for at this time, the United States will use various fora (i e , international alliances of private businesses, the International Organization for Standardization [ISO], the International Electrotechnical Commission [IEC], International Telecommunications Union [ITU], etc ) to discourage the use of standards to erect barriers to free trade on the developing GII The private sector should assert global leadership to address standards setting needs The United States will work through intergovernmental organizations as needed to monitor and support private sector leadership

## A COORDINATED STRATEGY

The success of electronic commerce will require an effective partnership between the private and public sectors, with the private sector in the lead Government participation must be coherent and cautious, avoiding the contradictions and confusions that can sometimes arise when different governmental agencies individually assert authority too vigorously and operate without coordination

The variety of issues being raised, the interaction among them, and the disparate fora in which they are being addressed will necessitate a coordinated, targeted governmental approach to avoid

inefficiencies and duplication in developing and reviewing policy

An interagency team will continue to meet in order to monitor progress and update this strategy as events unfold Sufficient resources will be committed to allow rapid and effective policy implementation

The process of further developing and implementing the strategy set forth in this paper is as important as the content of the paper itself The U S Government will consult openly and often, with groups representing industry, consumers and Internet users, Congress, state and local governments, foreign governments, and international organizations as we seek to update and implement this paper in the coming years

Private sector leadership accounts for the explosive growth of the Internet today, and the success of electronic commerce will depend on continued private sector leadership Accordingly, the Administration also will encourage the creation of private fora to take the lead in areas requiring self-regulation such as privacy, content ratings, and consumer protection and in areas such as standards development, commercial code, and fostering interoperability

The strategy outlined in this paper will be updated and new releases will be issued as changes in technology and the marketplace teach us more about how to set the optimal environment in which electronic commerce and community can flourish

There is a great opportunity for commercial activity on the Internet If the private sector and governments act appropriately, this opportunity can be realized for the benefit of all people

---

**NOTES:**

1 The Administration's concept of the Global Information Infrastructure (GII) includes wired and wireless networks, information appliances such as computers, set-top boxes, video phones, and personal digital assistants, all of the information, applications and services accessible over these networks, and the skills required to build, design and use these information and communications technologies The Internet is a global matrix of interconnected computer networks using the Internet Protocol (IP) to communicate with each other For simplicity, the term "Internet" is used throughout this paper to encompass all such data networks and hundreds of applications such as the World Wide Web and e-mail that run on those networks, even though some electronic commerce activities may take place on proprietary or other networks that are not technically part of the Internet The term "online service provider" is used to refer to companies and nongovernmental institutions such as libraries and schools that provide access to the Internet and other online services, and groups that create content that is delivered over those networks

2 The Administration has directed federal agencies to employ digital communications tools in their day to day operations Examples include enabling students to apply for and receive federal college loans online, automating and streamlining federal procurement or grant applications, and providing small business owners with information and guidance about business opportunities overseas See "Government Information Technology Board, Access America", *formalized by* Executive Order *Federal Information Technology* (July 6, 1996)

3 "Bureau of Economic Analysis, U S Department of Commerce, Survey of Private Services

Transactions" (Nov 1996) The estimate covers 1995 and does not include transactions between affiliated companies, which could add as much as $47 billion in additional exports

4 Such commercial activity already has begun, with 1995 sales estimated at $200 million *See* "American Electronics Association/American University, Internet Commerce" (Sept 1996)

5 Recognizing the important role that government can play, the Administration already has provided strong support for the development of the GII In 1993, it issued a report entitled "NII Agenda for Action" The 1995 "GII Agenda for Cooperation" extended the vision of the National Information Infrastructure (NII) to a global platform

6 *E g*, the Committee on Payments and Settlement Systems of the Bank for International Settlements, the Basle Committee on Banking Supervision, and the Financial Action Task Force

7 NTIA concluded that opt-in consent (information cannot be used without the data subject's explicit authorization) is necessary for sensitive information, such as personally identifiable medical information, and opt-out consent (information may be used if the data subject does not explicitly say that it may not be used after meaningful notice) is sufficient for non-sensitive information Since publishing its report, NTIA has continued to investigate how the private sector can develop and implement meaningful self-regulatory regimes

8 For purposes of this paper, the term "telecommunications" encompasses voice telephony and data services, including information access technology

9 These principles were elaborated in "Global Information Infrastructure An Agenda for Cooperation," released by the Administration in February, 1995

10 Examples include government support for 6bone, an IPv6 testbed, DARPA's support for CommerceNet, the World Wide Web Consortium, and research on multicast and quality of service, NSF's support for the Lightweight Directory Access Protocol, and NIST's development of tools for testing compliance with the Virtual Reality Modeling Language (VRML) standard

Administration Statement on Commercial Encryption Policy

# Administration Statement on Commercial Encryption Policy

**July 12, 1996**

---

The Clinton Administration is proposing a framework that will encourage the use of strong encryption in commerce and private communications while protecting the public safety and national security It would be developed by industry and will be available for both domestic and international use

The framework will permit U S industry to take advantage of advances in technology pioneered in this country, and to compete effectively in the rapidly changing international marketplace of communications, computer networks, and software Retaining U S industry's leadership in the global information technology market is of longstanding importance to the Clinton Administration

The framework will ensure that everyone who communicates or stores information electronically can protect his or her privacy from prying eyes and ears as well as against theft of, or tampering with, their data The framework is voluntary, any American will remain free to use any encryption system domestically

The framework is based on a global key management infrastructure that supports digital signatures and confidentiality Trusted private sector parties will verify digital signatures and also will hold spare keys to confidential data Those keys could be obtained only by persons or entities that have lost the key to their own encrypted data, or by law enforcement officials acting under proper authority It represents a flexible approach to expanding the use of strong encryption in the private sector

This framework will encourage commerce both here and abroad It is similar to the approach other countries are taking, and will permit nations to establish an internationally interoperable key management infrastructure with rules for access appropriate to each country's needs and consistent with law enforcement agreements Administration officials are currently working with other nations to develop the framework for that infrastructure

In the expectation of industry action to develop this framework internationally, and recognizing that this development will take time, the Administration intends to take action in the near term to facilitate the transition to the key management infrastructure

The measures the Administration is considering include

1 Liberalizing export controls for certain commercial encryption products

2 Developing, in cooperation with industry, performance standards for key recovery systems and products that will be eligible for general export licenses, and technical standards for products the government will purchase

3 Launching several key recovery pilot projects in cooperation with industry and involving international participation

4 Transferring export control jurisdiction over encryption products for commercial use from the Department of State to the Department of Commerce

Administration officials continue to discuss the details of these actions with experts from the communications equipment, computer hardware and software industries, civil liberties groups and other members of the public, to ensure that the final proposal balances industry actions towards the proposed framework, short-term liberalization initiatives, and public safety concerns

The Administration does not support the bills pending in Congress that would decontrol the export of commercial encryption products because of their serious negative impact on national security and law enforcement Immediate export decontrol by the U S could also adversely affect the security interests of our trading partners and lead them to control imports of U S commercial encryption products

A Cabinet Committee continues to address the details of this proposal The Committee intends to send detailed recommendations to the President by early September, including any recommendations for legislation and Executive Orders The Committee comprises the Secretaries of State, Defense, Commerce and Treasury, the Attorney General, the Directors of Central Intelligence and the Federal Bureau of Investigation, and senior representatives from the Office of the Vice President, the Office of Management and Budget, and the National Economic Council

# US Cryptography Policy:

## Why We Are Taking the Current Approach

**July 12, 1996**

We live in an age of electronic information Information technology is transforming society, creating new businesses, new jobs and new careers The technology also creates new opportunities for crime, and new problems in investigating and prosecuting crime As a result, electronic information, be it corporate trade secrets, pre-release government crop statistics, or a patient's medical records, must have strong protection from uninvited modifications of disclosure Cryptography enables that protection

The United States is the world leader in information technology US firms continue to dominate the US and global information systems market Retaining this leadership is important to our economic security The Clinton Administration, through its National Information Infrastructure initiative, has long recognized that government has an important role as a facilitator and catalyst for the industry-led transformation of the way we use computer and communications technology to work and live

In particular, government has a strong interest in promoting the legitimate use of robust encryption to support US international competitiveness, foster global electronic commerce, prevent computer

crime, and ensure that the information superhighway is a safe place to conduct one's business At the same time, there is a growing recognition, affirmed most recently by the National Academy of Science that the use of encryption to conceal illegitimate activities "poses a problem for society as a whole, not just for law enforcement and national security " In brief, criminals can use encryption to frustrate legal wiretaps and render useless search warrants for stored electronic data We know of no technical solution to the problems that would result from the global proliferation of strong cryptography (see box) The implications of this are no small matter

Encrypted computer files have hampered the prosecution of child pornographers Militia groups advise their members to use encryption to hide illicit weapons, financial, and other criminal activities Aldrich Ames was instructed by his Soviet handlers to encrypt computer files that he passed to the Soviets And international terrorists and drug dealers increasingly use encryption to prevent law enforcement officials from reading their voice and data transmissions Grave crimes, such as a plot to shoot down several airliners over Chicago, have been foiled by the use of wiretaps Had the FBI been unable to read those transmissions, however, a major tragedy might have ensued

No restrictions apply to the US domestic use of cryptography, and the Administration has no plan to seek restrictions Cryptography has long been controlled for export for national security reasons, so as to keep it from getting into the hands of foreign governments But is has today become a dual-use technology, and international businesses want to use the same security products both domestically and abroad The Administration is thus under strong pressure to provide relief from cryptography export controls

For our cryptography policy to succeed, it must be aligned with commercial market forces and operate on an international basis Further, it should preserve and extend the strong position that US industry enjoys in the global information systems marketplace Accordingly, the US government is working with US industry and our international trading partners on an approach that will protect information used in legitimate activities, assure the continued safety of Americans from enemies both foreign and domestic, and preserve the ability of the US information systems industry to compete worldwide

**Key Management and Recovery**

A consensus is emerging around the vision of a global cryptography system that permits the use of any encryption method the user chooses, with a stored key to unlock it when necessary The encryption key would be provided voluntarily by a computer user to a trusted party who holds it for safe keeping This is what many people do with their house keys -- give them to a trusted neighbor who can produce them when something unexpected goes wrong Businesses should find this attractive because they do not want to lock up information and throw away the key or give an employee -- not the company -- control over company information An individual might also use this service to ensure that she can retrieve information stored years ago This will require a new infrastructure, consisting of trusted parties who have defined responsibilities to key owners Under law, these trusted emergency key recovery organizations would also respond in a timely manner to authorized requests from law enforcement officials who required the key to decode information lawfully obtained or seized from a subject of investigation or prosecution

The Federal government will use key recovery encryption on its own computers because it makes good management sense It would be irresponsible for agencies to store critical records without key recovery, risking the loss of the information for programmatic use and the inability to investigate and prosecute fraud or misuse of the information

A number of US and international companies are working with the US and other governments to create a system of trusted parties who are certified to safeguard the keys In some cases, organizations might guard their own keys In other cases, persons will use the key recovery services provided by third parties, one of a suite of services that will include electronic directories and electronic "notaries" in support of online commerce Persons will be free to choose the type and strength of encryption that provide the degree of security they believe appropriate for their use Taken together, an overall key management infrastructure is needed to make electronic commerce practical on a global scale

Some commercial products and services which provide emergency key recovery are already available Testing and refinement is needed before a widespread, robust infrastructure is put in place The US government is committed to supporting the development of such a key management infrastructure through pilots and experimental trials The State Department is expediting the review of several export license applications that test commercial key recovery on an international scale An interagency working group is identifying several potential governmental uses of commercial cryptography - both internal transactions and in communications with the public - where key recovery can be tested A plan outlining these government tests will be available in August The government will be purchasing key recovery products for its own use, and will adopt a Federal standard for evaluating such products to assure agency purchasers that the key recovery features operate properly The Department of Commerce will be establishing an industry-led advisory committee to make recommendations regarding such a standard this Summer

While we are open to other alternatives, a key recovery system is the only approach we know of that accommodates all public safety interests And even it is imperfect Some people will not join voluntary systems, preferring to run the risk of losing their keys and being unable to recover their encrypted information Although in some countries (e g , France) mandatory key escrowing is already in effect, we are pursuing a market-driven approach in part because we hope and believe that key recovery will develop as a cost-effective service in an electronic commerce infrastructure We are encourage in this effort by recent discussions we have had at the Organization for Economic Cooperation and Development (OECD) that are leading to international cryptography management principles which support key recovery

**Export Controls**

No matter how successful we are in realizing this vision, American users of computer technology are demanding stronger encryption for international use now Although we do not control the use of encryption within the US, we do, with some exceptions, limit the export of non-escrowed mass market encryption to products using a key length of 40 bits (The length of the encryption key is one way of measuring the strength of an encryption product Systems using longer keys are harder to decrypt ) US industry asserts that it is losing overseas sales to its European and Japanese competitors because it cannot include stronger cryptography as a component of its commercial software and hardware products It warns that loss of a significant share of the world information systems market would cause serious economic damage to the US economy, and could reduce the US government's ability to influence the long term future of global cryptography It also argues that because customers do not want to use one product in the US and a different one overseas, export controls are causing US firms to provide an unsatisfactory level of protection to their electronic information, making them vulnerable to industrial espionage by their competitors and foreign governments

While 40 bit encryption products are still strong enough for many uses, the Administration

recognizes that some export liberalization may be useful to build support for a key management regime Accordingly, we are actively considering measures that would provide limited, temporary relief from cryptographic export controls in exchange for real, measurable commitments from industry (e g , investments in products that support key recovery) toward the building of a key management infrastructure The liberalization proposals under discussion, which would continue the current one-time review of products by the National Security Agency, include permitting products using longer key lengths to be exported to specific industry sectors such as health care or insurance (similar to current policy for the financial sector), allowing export of non-escrowed products to a list of trustworthy firms beyond those sectors, with provisions for monitoring compliance to prevent product diversion to other firms, export of cryptography-ready operating systems, and, most dramatically, the transfer of jurisdiction over commercial encryption products from the State Department's munitions list to the Commerce Department's list of dual-use technologies Our goal is to obtain commitments from industry by the Fall

We must, however, be careful in any relaxation of controls Other governments' law enforcement and national security needs to access material encrypted with US products could drive them to erect trade barriers by imposing import controls on strong non-escrow encryption products In addition, we do not want to do anything that would damage our own national security or public safety by spreading unbreakable encryption, especially given the international nature of terrorism Even 40 bit encryption, if widespread and not escrowed, defeats law enforcement

It is for these reasons that we oppose the legislation (S 1726) introduced in this Congress by Senator Burns and co-sponsored by Senator Lott and former Senator Dole Although it contains some provisions, such as the transfer of export control jurisdiction for commercial cryptography to the Commerce Department, with which we could agree if constructed with appropriate safeguards the bill is unbalanced, and makes no effort to take into account the serious consequences of the proliferation it would permit

The importance of the US information technology industry, the security stakes, and increasing Congressional interest make it clear that there is an urgent need for clear policy and direction The Administration's proposed approach is broadly consistent with industry suggestions and conclusions reached by the National Academy of Sciences in its report That report recognizes the need to address a complex mix of commercial and security issues in a balanced manner We agree with that need We also agree with the report's recommendation that export controls on encryption products need to be relaxed but not eliminated, and are actively considering ways of providing short term relief (We do not agree with the report's recommendation that we eliminate most controls on 56-bit key length products ) Finally, we agree that key escrow is a promising but not fully tested solution, and are promoting the kinds of testing the report recommends as a way of demonstrating the solution's viability while providing stronger encryption internationally

We will continue discussion with industry, other members of the private sector, the Congress, and governments at all levels to arrive at a solution that promotes a future of safe computing in a safe society

**Sidebar: Cracking Coded Messages**

We should not underestimate how difficult is to decode encrypted electronic information One